Cyberspace Training - Is This Even Legal?

Dr. David “Fuzzy” Wells, Deputy Director, UCF Institute for Simulation and Training
Derek Bryan, USINDOPACOM J81/Ingenia Services, Inc.

INSTITUTE for SIMULATION & TRAINING

UNITED STATES INDO-PACIFIC COMMAND
CYBER WAR INNOVATION CENTER

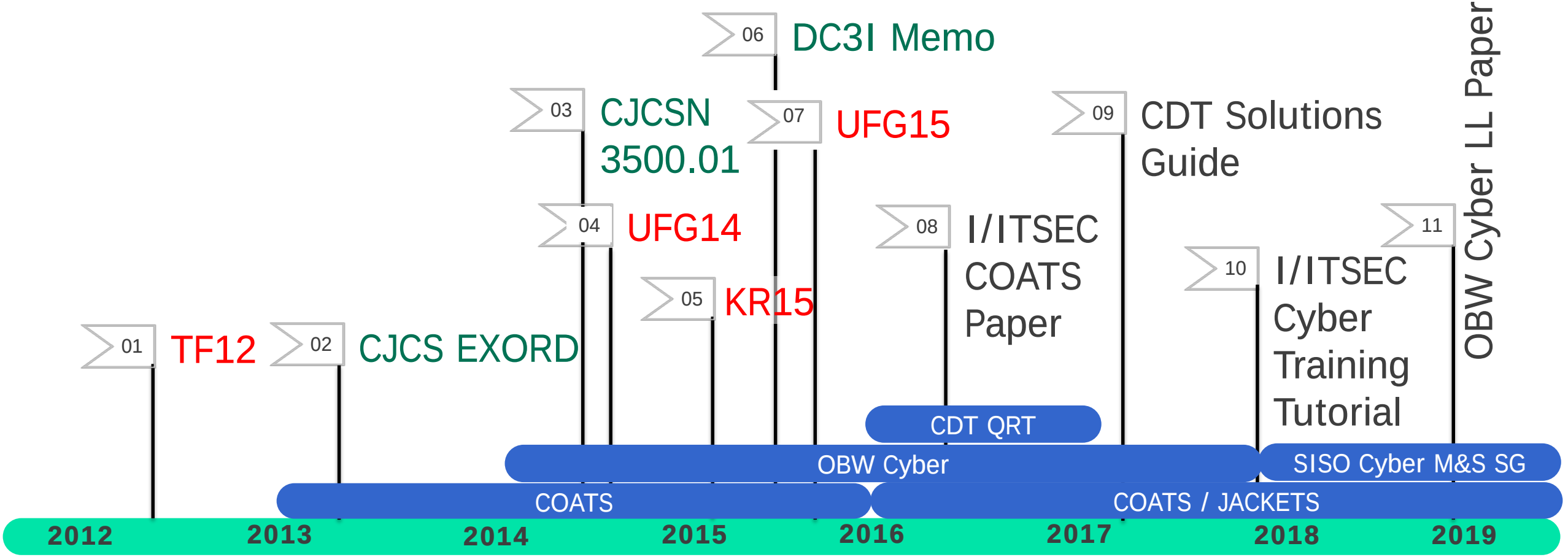
Workshop Outline

- Introduction
- Who Told You This Was a Good Idea?
- Know Your Training Audience and Their Expectations
- Cyberspace Training Concepts and Technologies
- Designing a Cyberspace Training Environment
- Demonstrations
- Current Challenges and the Future of Cyberspace Training
- Summary/Conclusion/Q&A

Introduction

- Learning Objectives
  - Describe government requirements and guidance for conducting cyberspace training
  - Define and describe key cyberspace training audiences and outcomes
  - Define and describe key cyberspace training concepts and technologies
  - Explain the process of designing a cyberspace training environment
  - Describe the current challenges and future of cyberspace training
  - Demonstrate and experience critical cyberspace training tools
- Intended Audience: This workshop will aid anyone involved with designing and executing cyber training events – leaders, planners, cyber warriors, service providers, and general users – who provide or rely on cyberspace capabilities to accomplish their mission

Introduction – How did we get here?



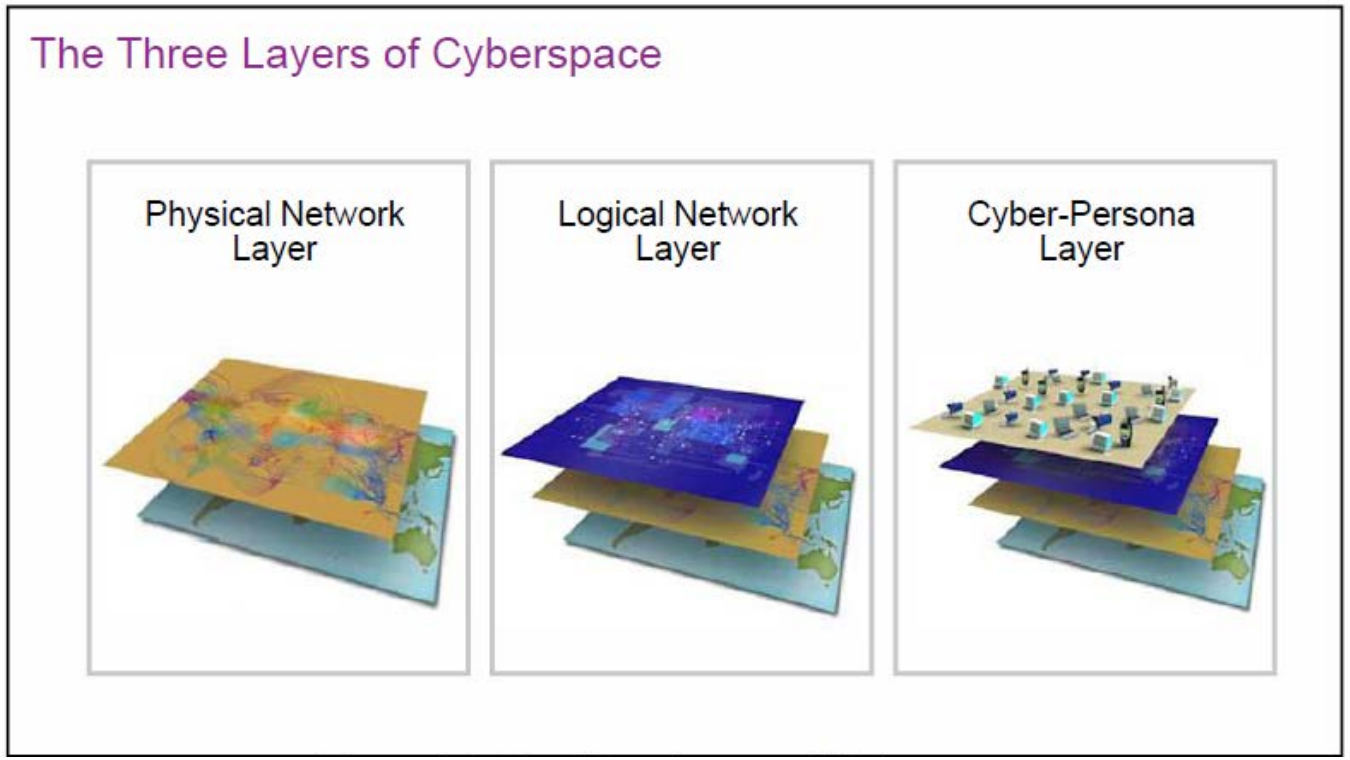
Introduction – Cyberspace Definitions

- Cyberspace – A global domain within the information environment consisting of the interdependent network of information technology, infrastructures, and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Joint Publication [JP] 1-02)

- Cyberspace Operations (CO) – The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Capabilities include, but are not limited to, Computer Network Exploitation (CNE), Computer Network Defense/Defensive Cyber Operations (CND/DCO), and Computer Network Attack/Offensive Cyber Operations (CNA/OCO). (JP 3-12)

Introduction – Cyberspace Definitions

- The **physical network layer** of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel.
- The **logical network layer** consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node.
- The **cyber-persona layer** represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network.



(JP 3-12)

Introduction – U.S. Cyber Mission Forces

Cyber National Mission Force (NMF)

Defend the Nation by seeing adversary activity, blocking attacks and maneuvering to defeat them

NMT

National Mission Team (NMT)

NST

National Support Team (NST)

Cyber Combat Mission Force (CMF)

Conduct military cyber operations in support of combatant commands

CMT

Combat Mission Team (CMT)

CST

Combat Support Team (CST)

Cyber Protection Force (CPF)

Defend DoD Information Networks (DODIN) and, when authorized, other infrastructure

CPT

Cyber Protection Team (CPT)

- ***National***
- ***CCMD***
- ***Service***

Introduction – Cyberspace Actions

- **Cyber attack** – Obvious functional denial, or manipulation that leads to denial in cyberspace or other domain.
- **Cyber Operational Preparation of the Environment (OPE)** – Prepare areas of cyberspace terrain for future operations.
- **Cyber Intelligence, Surveillance, Reconnaissance (ISR)** – Gather intelligence from target and adversary systems through cyberspace.
- **Cyber defense** – Detect, characterize, counter, and mitigate specific threat within a defended network. These are the actions we take when our cyber security has failed.
- **Cyber security** – Install, (re)configure, train, update, monitor, etc. in order to maintain configuration, integrity, and availability.

(Joint Concept for Cyberspace)

ATTACK	OPE	ISR	DEFENSE	SECURITY
• Degrade • Disrupt/Destroy • Deny • Manipulate/Exploit	• Non-intel • Plan & prepare for operations	• Intel gathering • Mapping • Surveilling	• Protect – Detect • Counter – Mitigate • Pro-active • Anticipatory	• Compliance • Scanning • Patching

Introduction – Cyberspace Techniques and Effects

- **Backdoor** – Access bypassing normal security, typically intentional to allow administrator or vendor access
- **Denial of Service (DOS)** – Disrupt network service by overwhelming system resulting in network slowing or crash
- **Distributed Denial of Service (DDOS)** – DOS using numerous computers and multiple paths
- **Phishing** – Spoofing of legitimate e-mail enticing recipient to take compromising action
- **IP Address Spoofing** – Hide true identity of source or destination; often used in DDOS attack
- **Keylogger** – Software or hardware monitoring and logging of user keystrokes often for password compromise
- **Logic Bomb** – Malicious software that destroys data by reformatting hard disk or inserting random data
- **Physical Attack** – Physical destruction of workstation, servers, transport or other terminal equipment
- **Sniffer** – Program or device monitoring data traversing a network to steal data or passwords
- **Trojan Horse** – Malicious program or utility that appears legitimate performing compromising background processes
- **Virus** – Software designed to infect, destroy, modify or cause other problems with computer or legitimate software
- **Worm** – Software designed to replicate across a network and delete, modify, improperly distribute, or manipulate data
- **Ransomware** – Malicious software blocking access to data until a ransom is paid; destroy data if not paid

(Strategic Cyberspace Operations Guide)

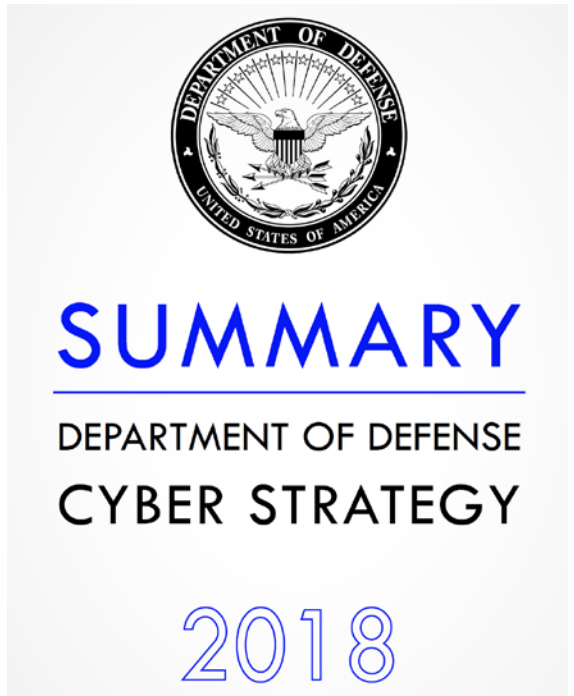
Introduction – Cyber Threats

- **Nation State Threat** – This threat is potentially the most dangerous because of access to resources, personnel, and time that may not be available to other actors. Nation states may conduct operations directly or may outsource them to third parties to achieve their goals.
- **Transnational Actor Threat** – Formal and informal organizations that are not bound by national borders.
- **Criminal Organization Threat** – May be national or transnational in nature. Criminal organizations steal information for their own use or, in turn, to sell to raise capital.
- **Individual Actors or Small Group Threat** – Gain access into systems to discover vulnerabilities, sometimes sharing the information with the owners; however, they also may have malicious intent.
- **Insider Threat** – Harmful acts that trusted insiders might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual.
- **Natural Threat** – Can damage and disrupt cyberspace including events such as floods, hurricanes, solar flares, lightning, and tornados.
- **Physical Threat** – Physical threats to cyberspace and cyberspace operations such as a backhoe cutting a fiber optic cable of a key cyberspace node

(Strategic Cyberspace Operations Guide)

Who Told You This Was a Good Idea?

- U.S.
  - Oct 2018, Government Accounting Office Report: Weapons System Cybersecurity
  - Sep 2018, DOD Cyber Security Strategy
  - Jan 2018, DOT&E FY 2017 Annual Report
  - Jul 2017, DODI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
  - May 2017, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
  - Feb 2017, Defense Science Board Report
  - Sep 2015, Office of the Secretary of Defense Memo, DoD Cybersecurity Culture & Compliance Initiative
- International
  - Feb 2017, Tallinn Manual 2.0 - International Law Applicable to Cyber Operations
  - Multinational Cyber Defence Education and Training Program



Who Told You This Was a Good Idea?

- "In the Marine Corps they say that every Marine is a rifleman. I say that everyone in the {Department of Defense} is a cyber warrior." (VADM Nancy Norton, Director DISA, Commander Joint Force HQ DODIN, CyberCon 2018)
- "Nearly all major acquisition programs that were operationally tested between 2012 and 2017 had mission-critical cyber vulnerabilities that adversaries could compromise." (GAO Report: Weapon System Cybersecurity Oct 2018)
- "#1 Objective: Ensuring the Joint Force can achieve its missions in a contested cyberspace environment." (US DOD Cyber Strategy 2018)
- "Given dramatic increases in the ability of adversaries to disrupt, degrade or destroy cyberspace and space systems, it is essential that the Joint Force be able to operate effectively despite degradation to those systems. Greater resilience must be built into technical architectures, and the force must regularly train to operate in "worst case" degraded environments." (CJCS Capstone Concept for Joint Operations: Joint Force 2020)

Know Your Training Audience

Leaders

- Commanders, Directors, senior leaders, decision makers, etc.
- Ensure accountability, lead change, provide resources

Providers

- Government and industry Information Technology professionals
- Design, build, secure, maintain, and operate cyberspace infrastructure

Cyber Warriors

- Cyber Mission Forces, Red Teams, and other cyberspace defenders
- Deliver effects through cyberspace to achieve mission objectives

Users

- Service members and civilians who rely on cyberspace for mission assurance and mission success
- Expected to have basic understanding of cyberspace and exhibit good cyber hygiene

(DC3I)

Know Your Training Audience's Expectations

Leaders Opportunities to develop, evaluate, train, and exercise CONOPS/TTPs for full spectrum operations in contested environments	**Providers** Opportunities to evaluate, train, and exercise critical, inter-organizational capabilities and processes
Cyber Warriors Availability of credible, secure cyberspace environments for developing, evaluating, training, and exercising cyberspace CONOPS, TTPs, and material solutions	**Users** Opportunities to develop, evaluate, train, and exercise CONOPS/TTPs for integrated cyberspace operations, mission assurance, and continuity of operations

Training Concepts and Technologies – Terminology

- Live – Actual real-world assets operating on/with real-world systems and protocols; vulnerable and reachable by attacks, exploits, and performance degradation from the physical and/or simulated domains.
  - Real operators, real network devices, real machines, real non-emulated/simulated software
  - Packet, protocol, or frequency level attack and response launched by real systems and/or live attackers

Training Concepts and Technologies – Terminology

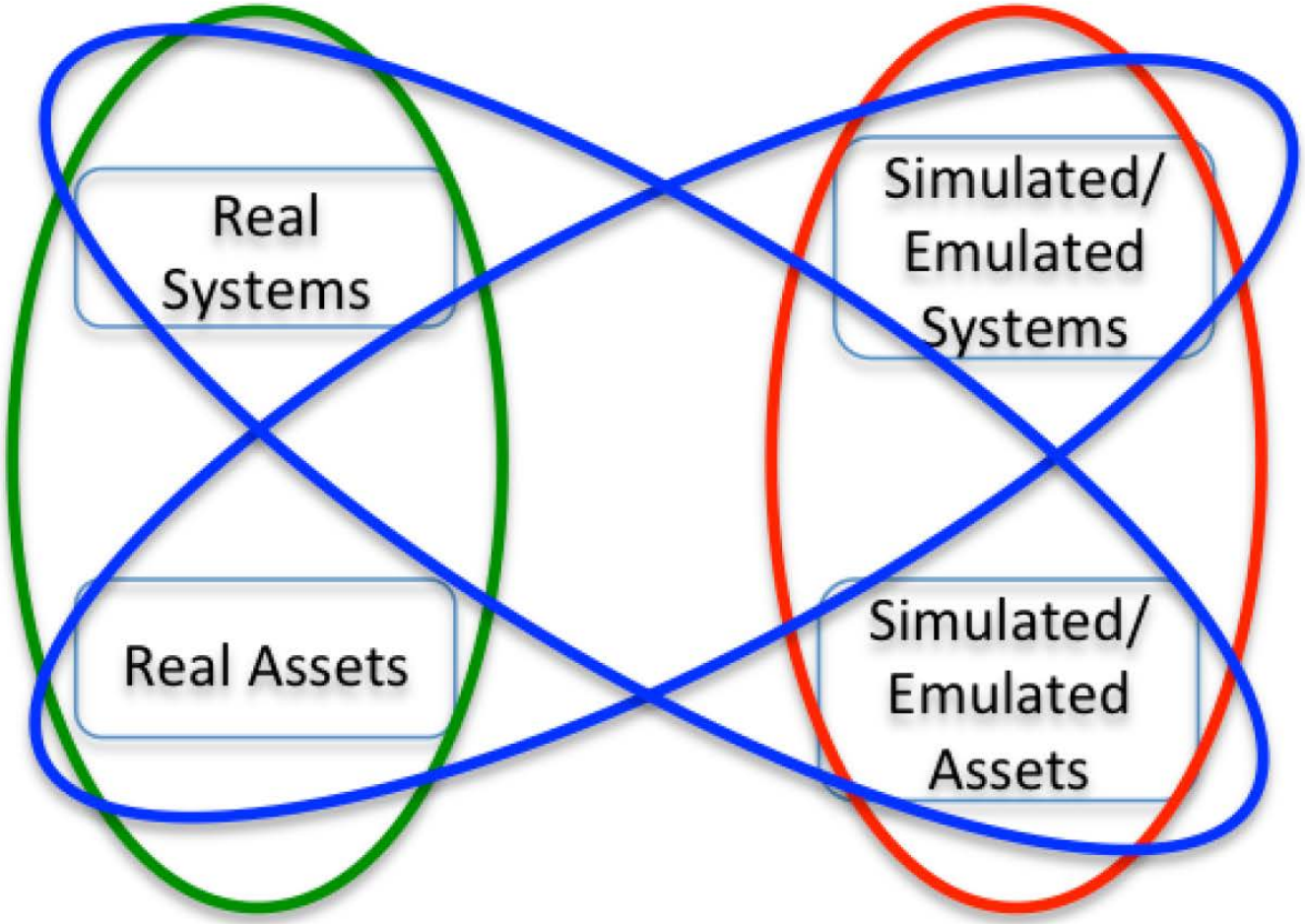
- Virtual – Protocol-level fidelity representations of real-world assets where ease of (re)configuration, replication, restoration and physical limitations make a virtual asset preferred over the live one. There is no physical representation of the real-world system, so a virtual asset only provides a cyber "attack surface," i.e. protocol/packet interfaces, but not asset internals susceptible to attack.
  - Asset emulators running on virtual machines
  - Automated response of a virtual machine to an attack
  - Replay of a logged live attack onto the live or virtual systems
  - Automated or semi-automated attack simulators that replicate the actions of a live red team or real world threat
  - Accurate (high-fidelity) representations of IA or sysadmin GUIs

Training Concepts and Technologies – Terminology

- Constructive – Parameterized simulated or emulated assets operating on/with simulated systems, but not vulnerable to direct live or virtual exploits and manipulation; characterized by low fidelity global/enterprise-level network and effects representations
  - Simulated internet-scale traffic generation, background noise and high-volume gray-space
  - Virus infection & worm propagation simulations
  - Asset representations with simulation interfaces, e.g. HLA FOMs, vs. packet/protocol interfaces
    - That must be translated or bridged to connect with virtual and live assets

Training Concepts and Technologies – Solutions Overview

- Computer-Based Training
- White Cards
- Tabletop Exercises
- Cyber Effects Emulations
- Cyber M&S
- Cyber Ranges
- Red Teams
- Integrated Environments



Training Concepts and Technologies – Computer-Based Training

- Provides individuals with the fundamental knowledge and skills necessary to perform basic tasks
- Often conducted prior to a larger event/exercise to ensure baseline knowledge and performance standards
- Potential cyberspace training applications:
  - Cyber security awareness
  - Insider threat
  - Cyber effects request
  - Threat vectors

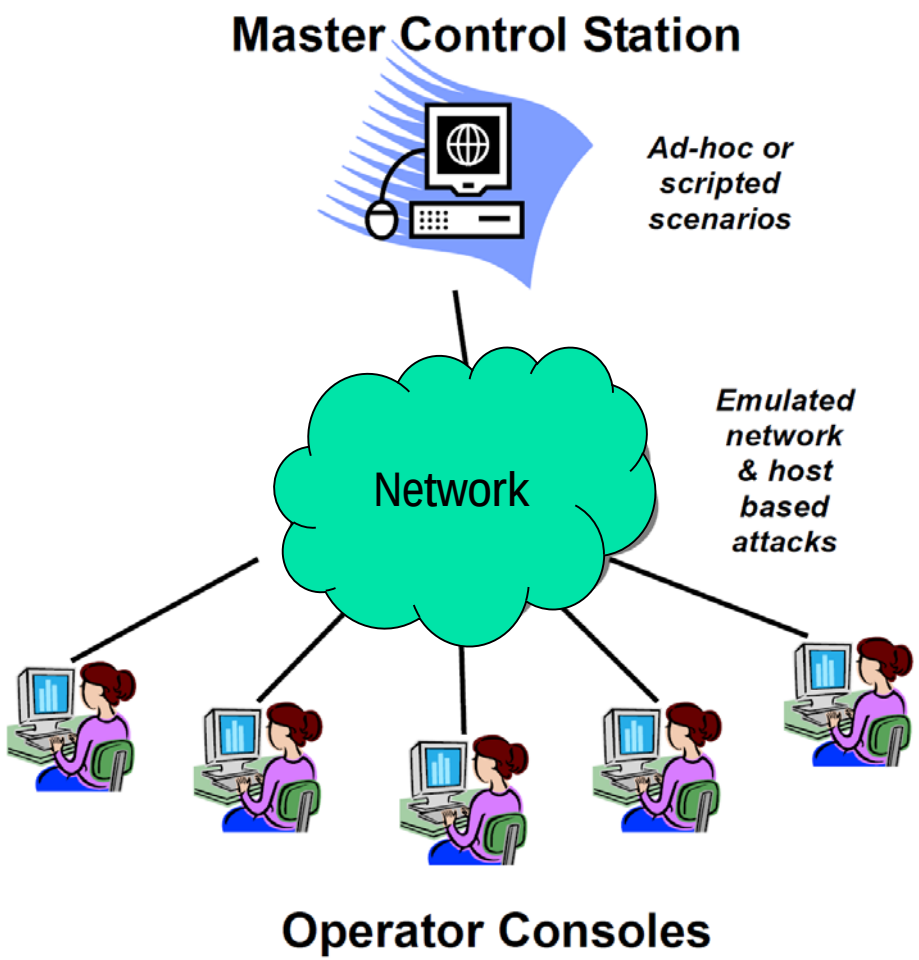
Training Concepts and Technologies – White Cards

- Static method for sharing cyber effects information with the training audience
- Expected to generate a training audience action/response
- Pros
  - Easy to integrate and implement as part of an exercise Master Scenario Event List (MSEL)
  - Can represent effects that cannot be represented using other methods
- Cons
  - No opportunity to realistically experience, interact with, or detect the event

Training Concepts and Technologies – Tabletop Exercises

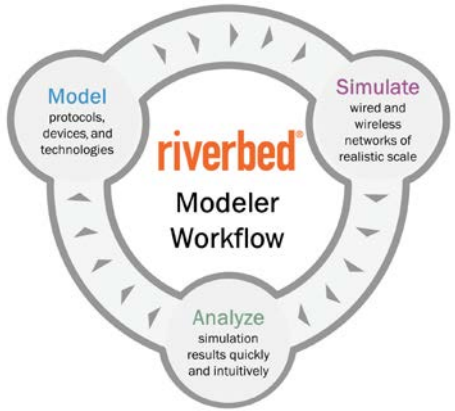
- Provides opportunities for teams to develop, learn, and share concepts, roles and responsibilities, and processes for common interests
- Often facilitated by a subject matter expert and executed under a representative operational context/scenario
- Potential cyberspace training applications:
  - Cyber command and control
  - Integrated cyber-kinetic operations
  - Mission assurance in contested environments

Training Concepts and Technologies – Cyber Effects Emulators



- Emulation of host and network cyber effects on operational systems:
  - HW/SW malfunction
  - Virus/malware/phishing
  - Network performance degradation
- Do not degrade or damage the underlying infrastructure; positive C2 of effects from remote workstation in exercise control group
- Pros
  - Easy to integrate and implement
  - More fidelity than white cards, less risky than red teams
- Cons
  - Information assurance on operational networks/systems
  - Minimal opportunities for network defender training

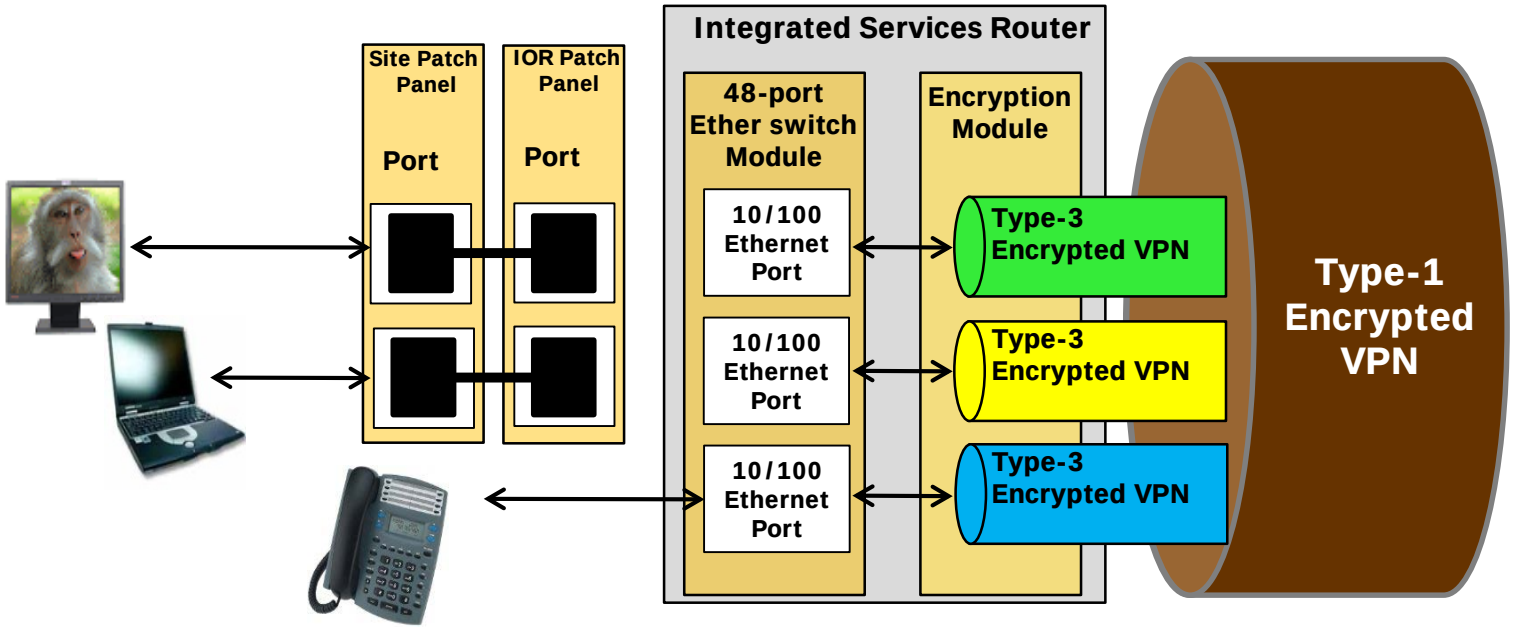
Training Concepts and Technologies – Cyber M&S



- Virtual and constructive representations of critical networks, nodes, systems and message traffic correlated with the overall exercise scenario and forces
- Should be planned, designed, tested, and executed similar to, and in concert with, traditional/kinetic M&S solutions

Training Concepts and Technologies – Cyber Ranges

- Cyber Range – A designated set of capabilities which can be integrated to generate an environment with the appropriate classification levels and controls to conduct research, development, demonstration, testing, or evaluation of military capabilities supported in, through, and from cyberspace, or to train military personnel in conducting cyber operations. Typically logically and/or physically separate from traditional training environments.



Training Concepts and Technologies – Red Teams

- "A group of DoD personnel authorized and organized to emulate a potential adversary's exploitation or attack capabilities against a targeted mission or capability." (CJCSM 6510.03)
- NSA-certified DoD red teams:
  - Vulnerability identification
  - Close action teams
  - Persistent cyber opposing forces
- Pros
  - High-fidelity representation of adversary
  - Responsive to emerging threats
- Cons
  - Limited resource
  - Planning intensive
  - Reconstitution

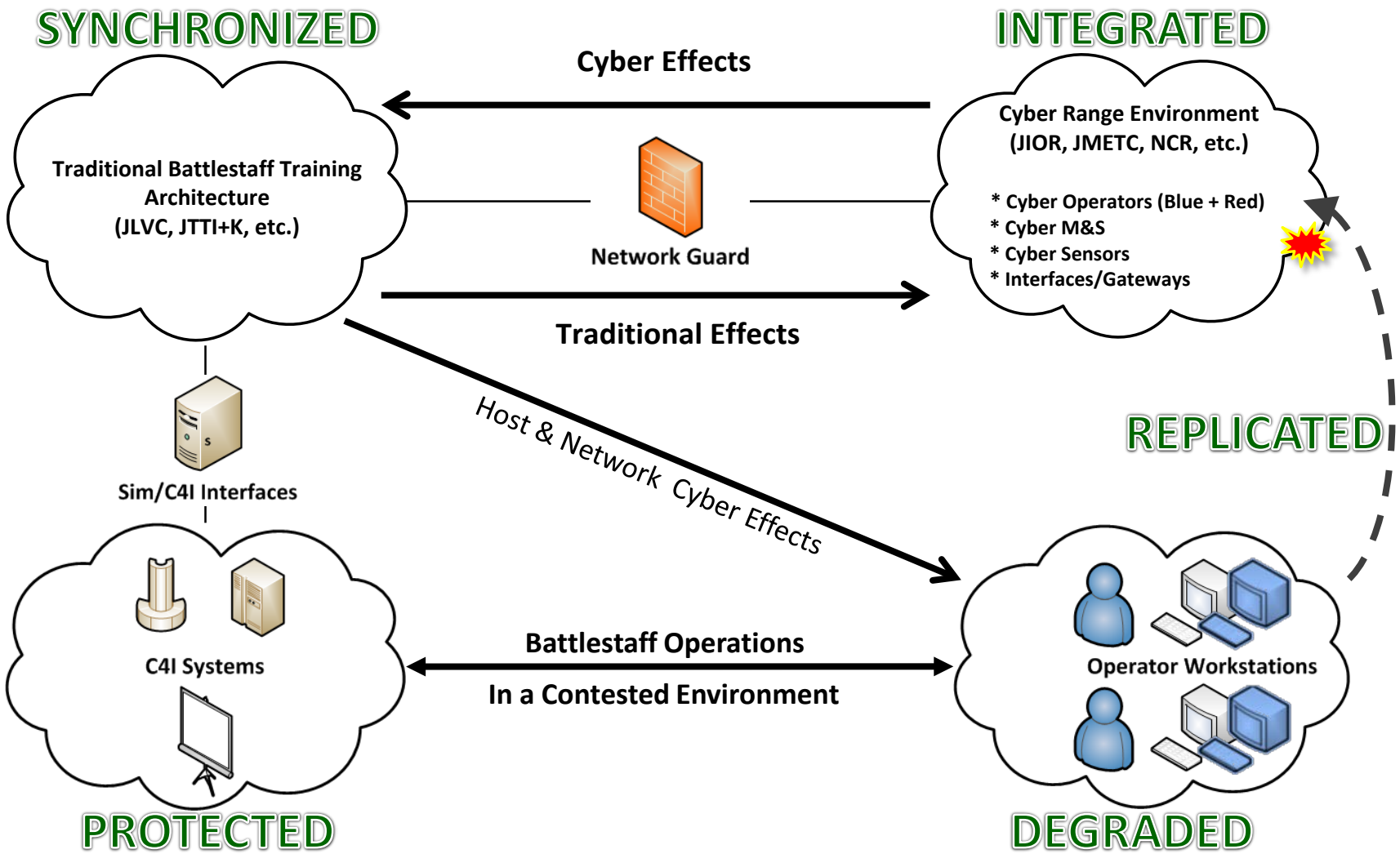
Training Concepts and Technologies – Integrated Environments

- Emerging capabilities for conducting integrated cyber-kinetic operations training
- Requires development and integration of cyber-kinetic interoperability methods and capabilities
- Recent Examples:
  - Cyber Operational Architecture Training System (COATS) / Op Blended Warrior (OBW) / Fleet Synthetic Training (FST)
  - Cyber Operations Battlefield Web Services (COBWebS)
  - Cyber-Kinetic Effects Integration (CKEI)
- Much work to be done to fully enable integrated cyber-kinetic operations training:
  - Standards development
  - Cyber-aware kinetic LVC capabilities
  - Kinetic-aware cyber LVC capabilities
  - Command and control of integrated cyber-kinetic training environments

Training Concepts and Technologies – CyRDEM

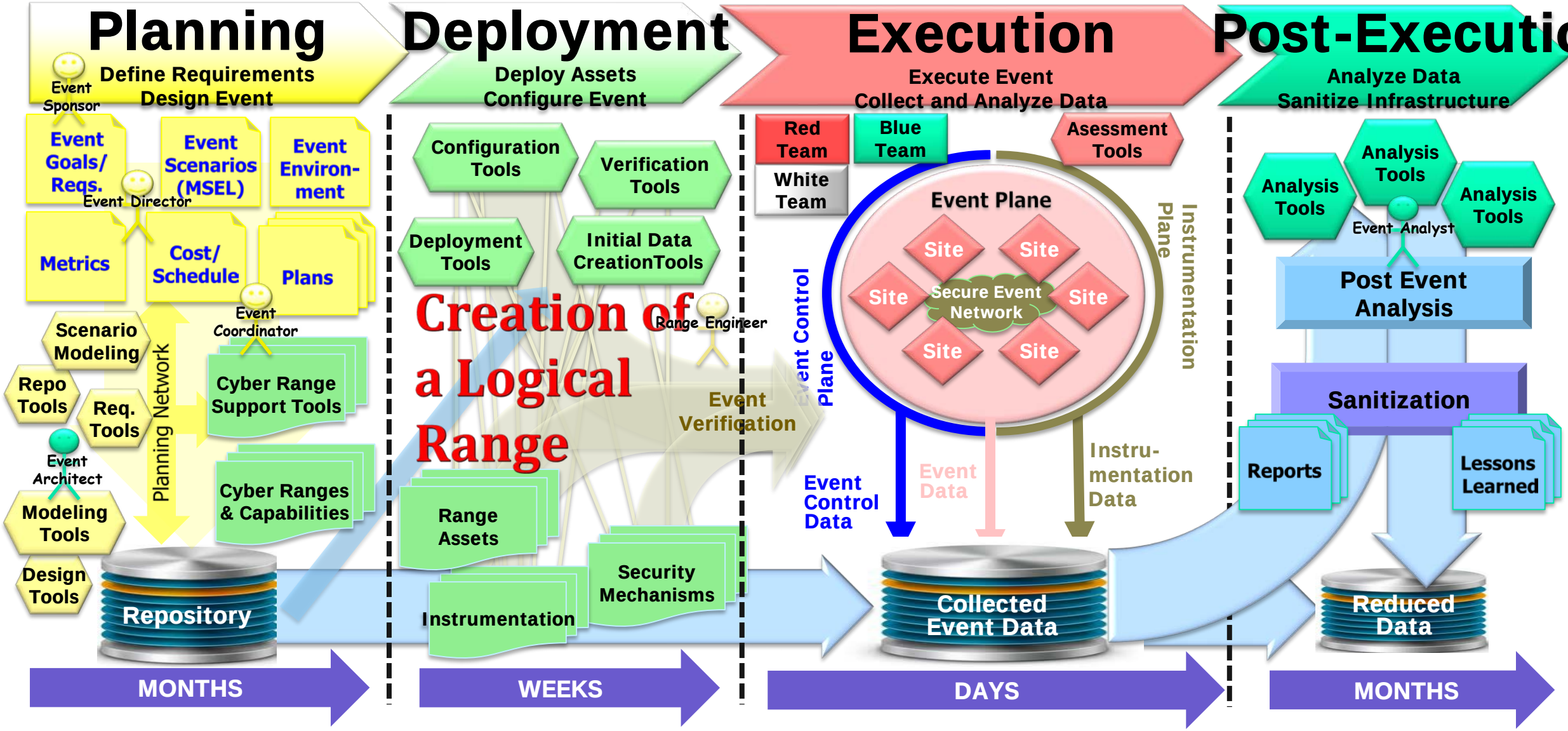
- The Cyber Reference Data Exchange Model (CyRDEM) CyRDEM is a protocol-agnostic representation of cyber objects and effects (not attacks) for distributed simulations
- The CyRDEM is not a standard. There is no standard for cyber effects information sharing in distributed simulation.
- To date the CyRDEM has been implemented in XML (ACE-IOS, NE2S) and HLA (JSAF, JBUS)
- Join the Simulation Interoperability Standards Organization's (SISO) Cyber M&S Study Group to help define this future standard.

Training Concepts and Technologies – COATS / OBW / FST



- Secure, controlled architecture for conducting integrated cyber-kinetic operations during battle staff exercises
- Leverages and enhances existing LVC capabilities – simulations, emulations, cyber ranges, controlled interfaces, etc.
- Event Support:
  - COATS – Pacific-theater exercises
  - OBW 2015, 2016, 2017 – Integrate cyber-degraded effects into government, industry, and academic training systems
  - FST RDT&E 2016, 2017 – Integrate cyber-degraded effects onto Navy tactical platforms

Training Concepts and Technologies – Cyber Range Event Process



@IITSEC NTSAToday

Joint Exercise Life Cycle Considerations

Planning Milestone	Traditional Training Environment	Cyberspace Training Environment
Concept Development	Obtain Commander's guidance	
	Design exercise construct	
Initial Planning	Develop and validate training objectives	
	Design training environment	
Mid Planning	Develop training events and measures	
	Develop training environment	
Final Planning	Finalize training events and measures	
	Test training environment	
Execution	Execute training environment and monitor trainee performance	
Assessment	Assess trainee performance and report results	

SAME

- Cyberspace training environments should be planned, designed, tested, and executed similar to, and in concert with, traditional/kinetic M&S solutions. No need to create a new or different process.

Designing a Cyberspace Training Environment

- Identify training audience and objectives
  - **Training Audience** – Leaders? Providers? Cyber Warriors? Users? Combination?
  - **Training Objectives** – CND/DCO? CNA/OCO? Mission Assurance? Continuity of Operations?

- Evaluate risk tolerance and available resources
  - **Risk** – To cyberspace training audience, to rest of exercise, to operational resources, etc.
  - **Resources** – Time, money, manpower, etc.

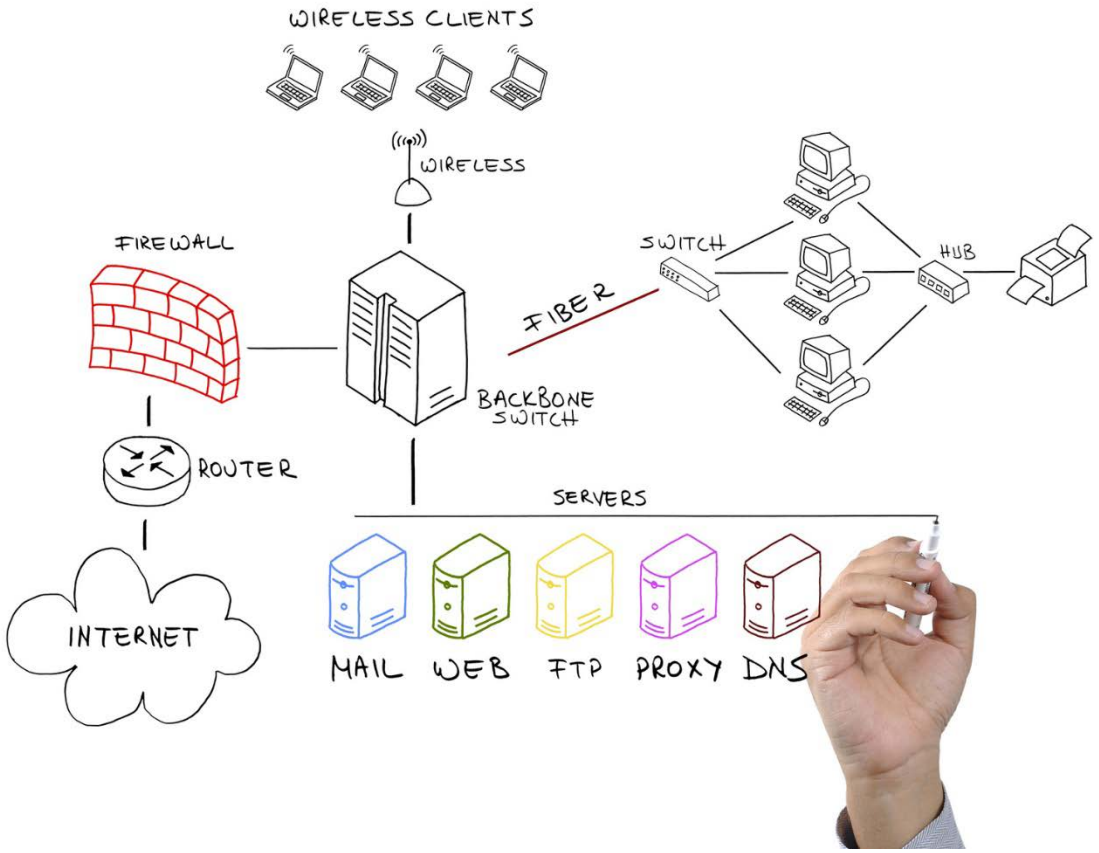
Designing a Cyberspace Training Environment

Audience	Focus	Cyber LVC Options
Individuals (All)	Cyberspace Awareness & Knowledge	CBT, White Cards, Cyber Effects Emulators
Individuals (Cyber)	Cyberspace Skills Development	CBT, Cyber M&S, Cyber Ranges
Teams (All)	CONOP/TTP Development and Evaluation	White Cards, Tabletop Exercises
	Exercise Integrated Cyberspace Operations	Integrated Environments
Teams (Non-Cyber)	Exercise operations in Contested Environments, Mission Assurance, and Continuity of Operations	White Cards, Cyber Effects Emulators, Cyber M&S, Red Teams, Integrated Environments
Teams (Cyber)	Cyberspace Skills Development	Cyber M&S, Cyber Ranges, Red Teams

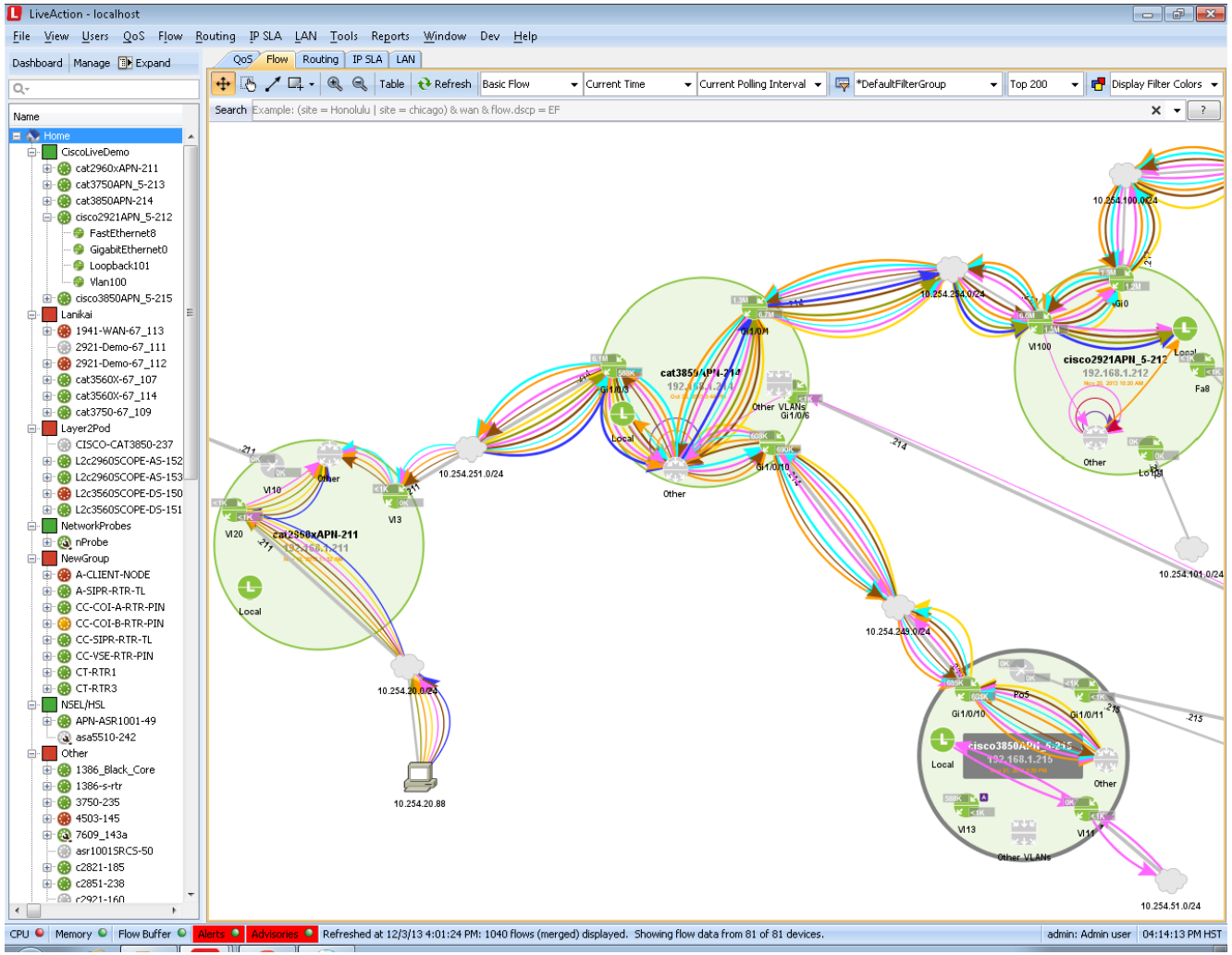
- In general, increased levels of fidelity/realism in your Cyber LVC environment will increase cost and potentially risk
- Recommend the lowest fidelity solution that meets requirements and limits risk

Designing a Cyberspace Training Environment

- Develop vignettes and supporting materials
  - **Road to Crisis** – How did we get here? What could happen next? What assumptions, limitations, and constraints apply?
  - **Key Cyber Terrain** – What Red, Blue, and other networks, systems, applications, and data apply? What capabilities are "off limits" (a.k.a. white list)?
  - **Set Initial Conditions** – Configurations, users, databases, etc. that increase the realism of the environment
  - **Response Cells** – Who do players interact with outside of the audience? Where do they get orders from? Who do they provide reports or orders to?



Designing a Cyberspace Training Environment



- Stimulate your audience to react
  - **Traffic Generation** – Network, system, device, application, user
  - **Indications and Warnings** – Sensors and intelligence
  - **Reports** – Government, industry, academia, traditional/social media
  - **White Cell** – When all else fails
- Shot validation & after-action review
  - **Observers/Trainers** – Qualitative
  - **Sensors** – Quantitative
  - **Data Collection and Analysis** – Reflective

10 Minute Break

Demonstrations / Presentations

- CyberBOSS, CyberCENTS, COBWebS
- iSCORE
- C2SIM
- TENA Retina
- NE2S

U.S. Army Research, Development and Engineering Command:

CyberBOSS / CyberCENTS / COBWebS Capability Demo

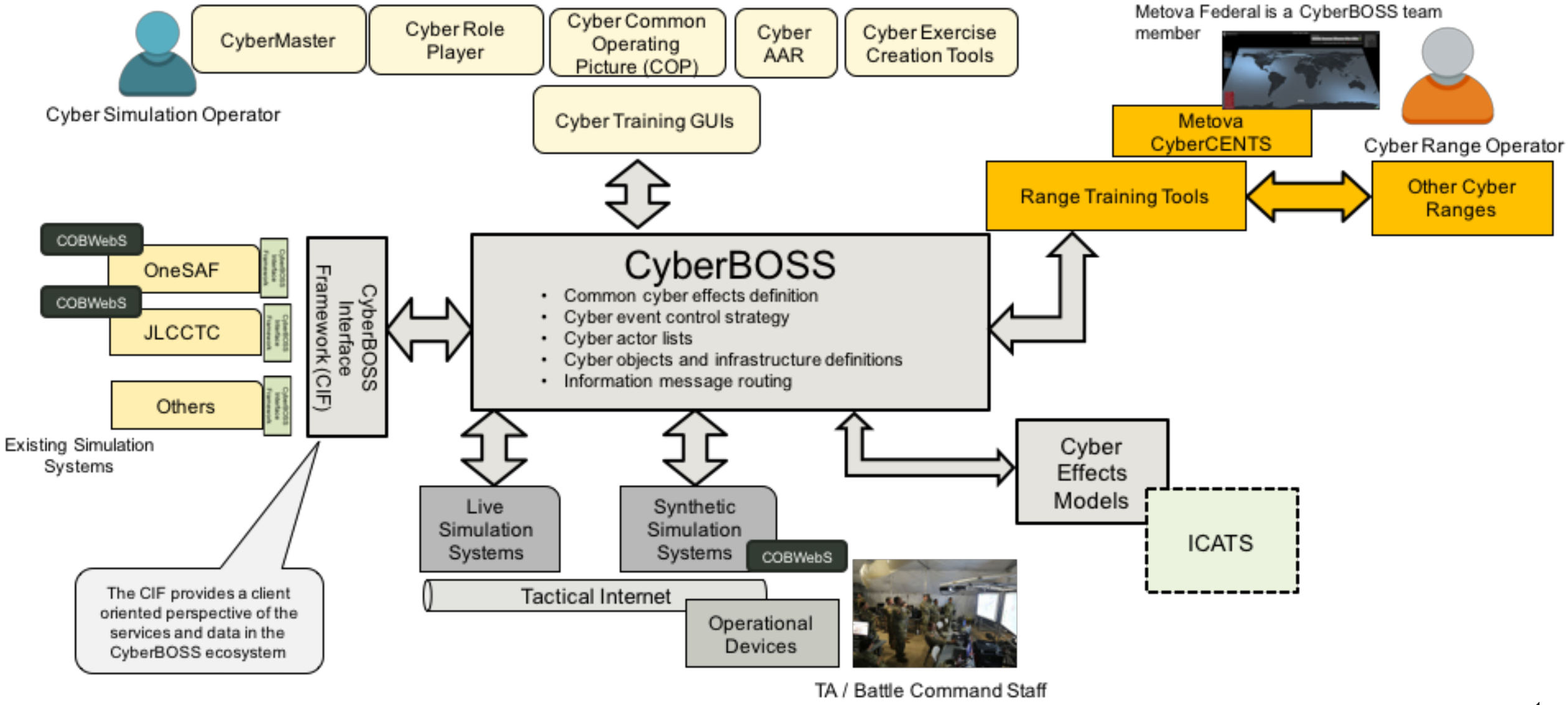
Bob Burch, Chief Technology Officer: Dignitas Technologies, LLC

Kevin Hofstra, Chief Technology Officer: Metova CyberCENTS

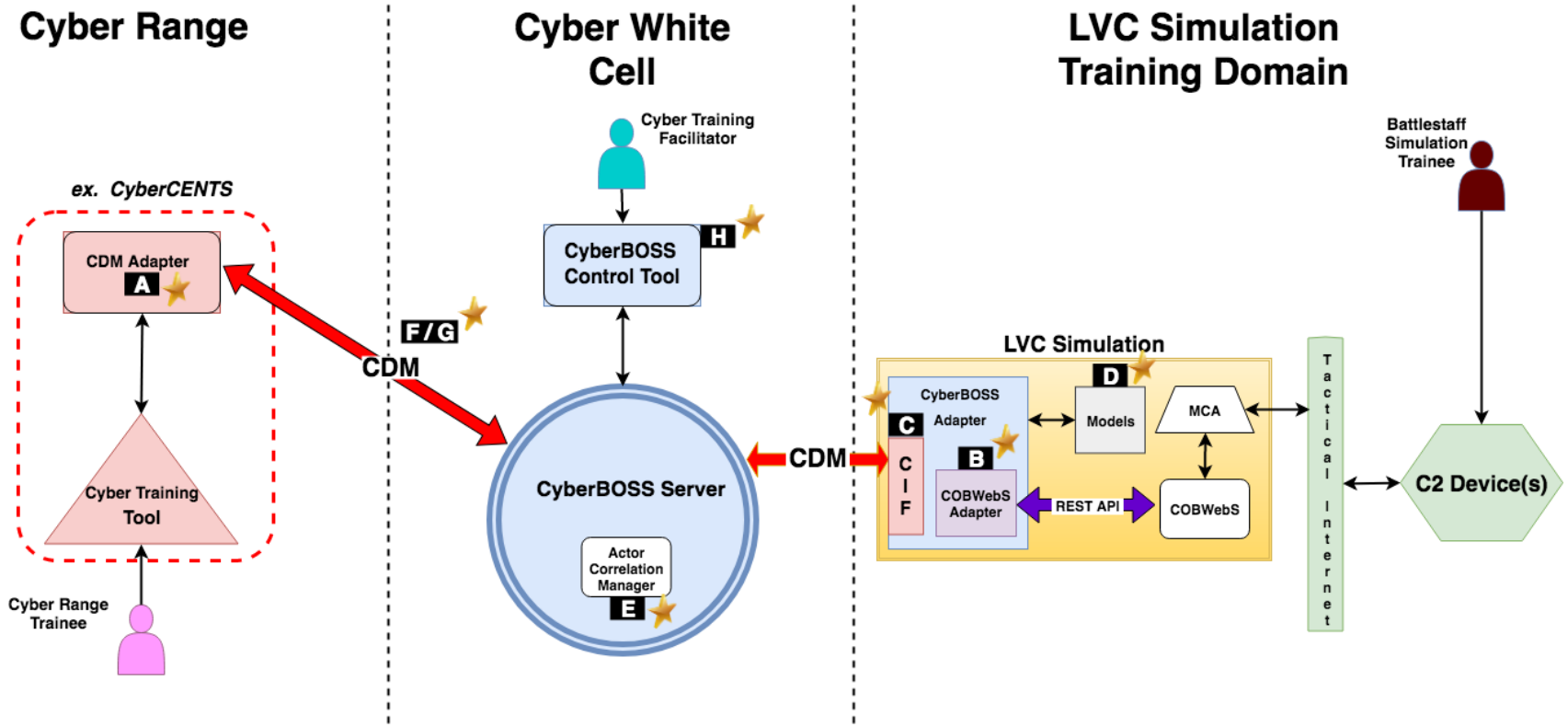
CyberBOSS Objectives

- Facilitate cyber effects and actions across LVC&G systems
- Develop a cyber terrain ecosystem that is more than a point solution
  - Open and transparent – easy for others to see what is happening internally
  - Flexible and extensible – adapt to future needs and facilitate third party extension
- Services approach with a transparent message passing scheme
  - Makes it easy to incorporate and extend
- Define a common data model for cyber intentions, cyber attacks and cyber control
  - JSON over the wire for accessibility
  - Leverage existing models (e.g., COATS)
- Correlation of cyber terrain between synthetic battlespace (LVC&G) and Cyber Range (Metova CyberCENTS)

Central Control and Routing of Cyber Effects



CyberBOSS Architecture Components



A: Cyber Range Adapter

B: COBWebS Adapter

C: CyberBOSS Interface Framework (CIF)

D: Cyber Modeling Enhancements (OneSAF)

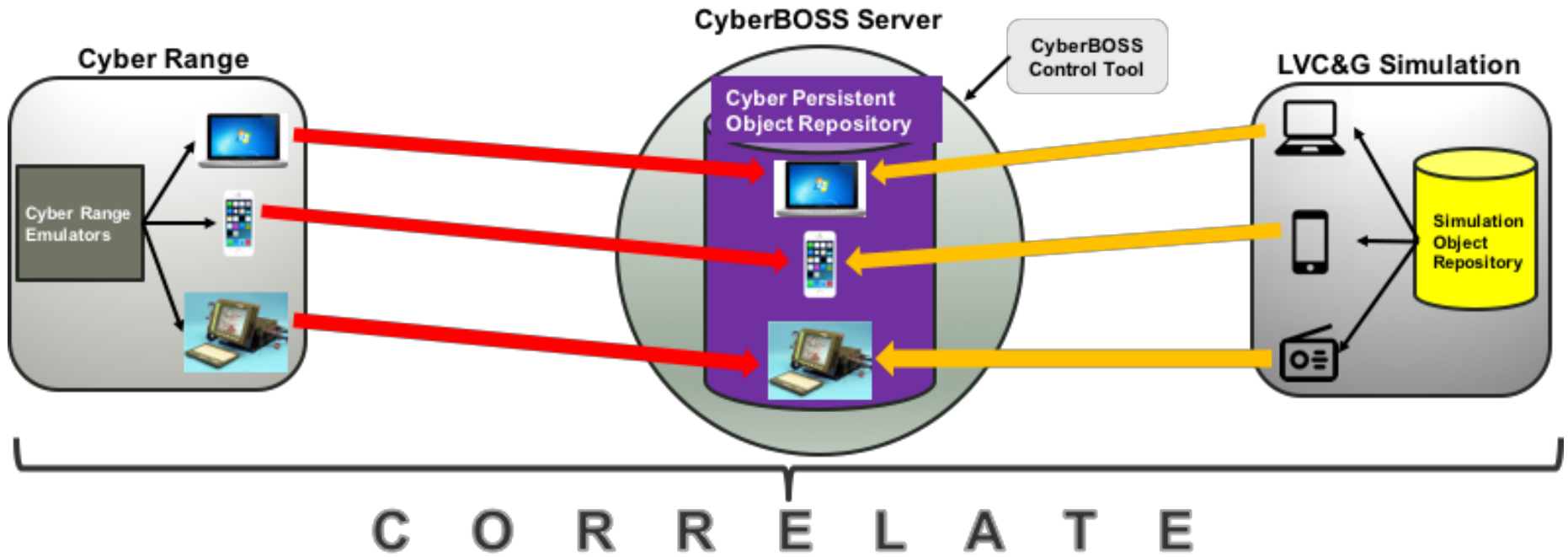
E: Correlation Management Services

F: CDM Data Model Enhancements

G: CDM Documentation Generator

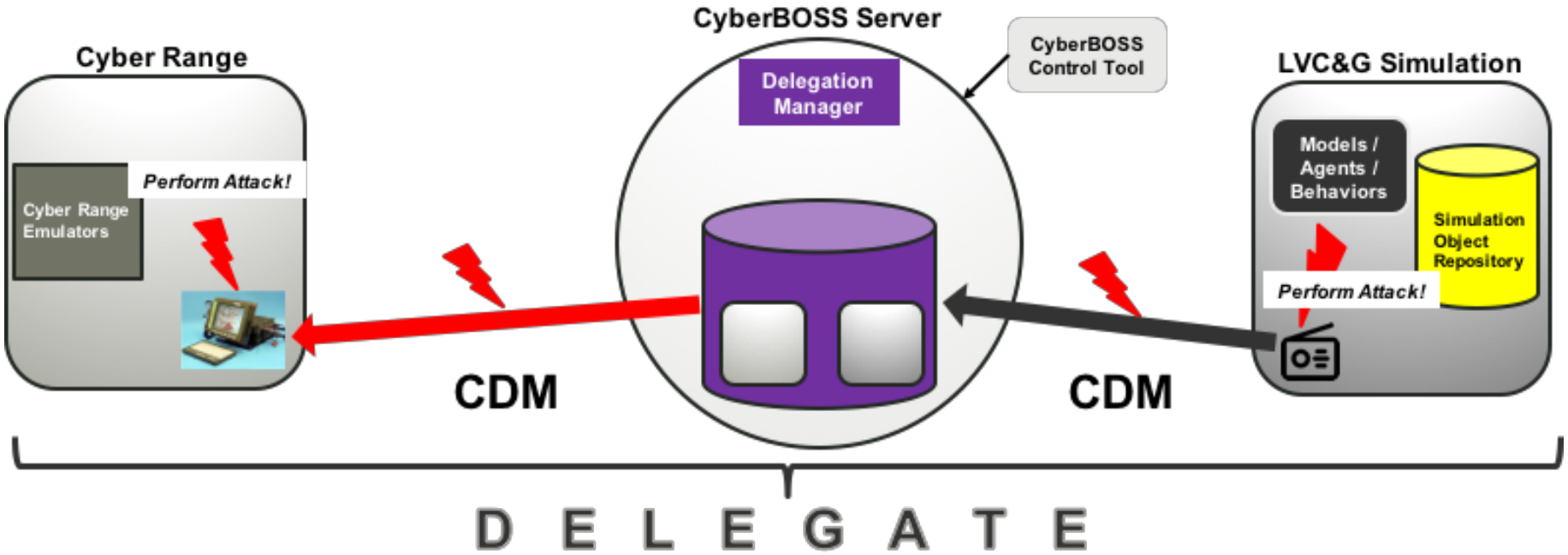
H: Control Tool Enhancements

Cross-Domain Device Correlation



- Disjoint representation of devices between CyberBOSS federates
  - The applications operate on different parameter sets, but refer to the same logical device
  - E.g., Cyber range provides device operating system & version, while LVC&G simulation provides location (tied to owning entity)
- CyberBOSS Server will correlate this data into a single, logical representation
  - Uses contextually relevant information from all federates to make adjudication decisions
  - This supports bridging effects on the devices between the connected applications
- THIS IS A KEY CAPABILITY OFFERED BY THE SYSTEM
  - Bridging device representations across multiple domains.

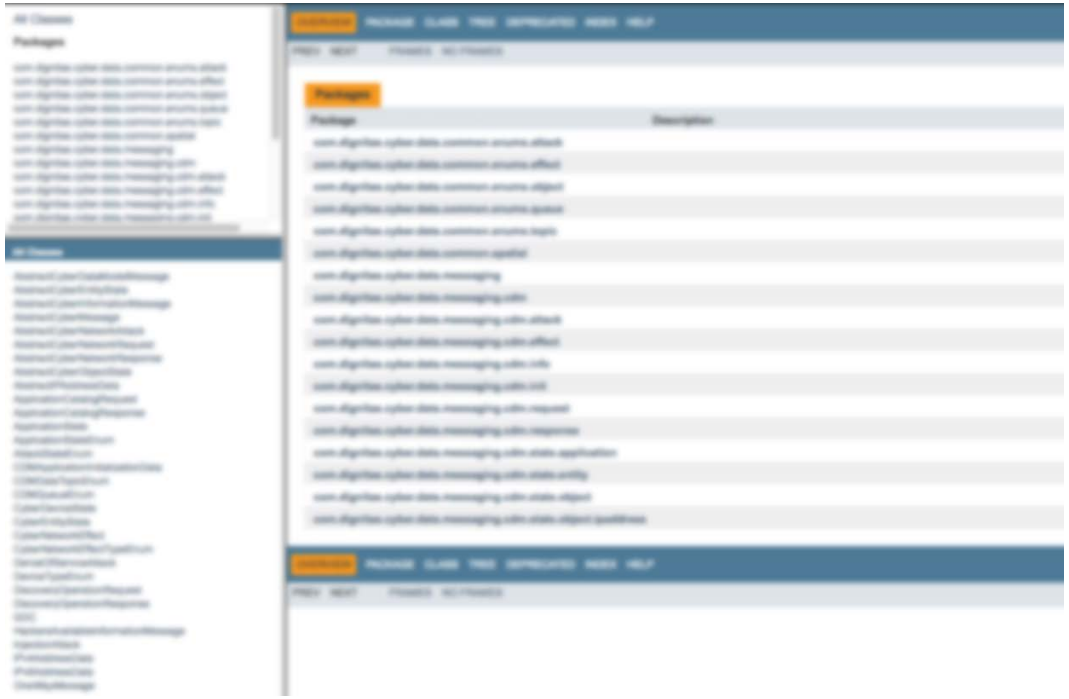
Cyber Event Delegation



- Harness correlated object representation to delegate requests
  - E.g., Task an actor in LVC&G simulation, delegate the work to another federate with higher fidelity representation.
- Adjudication / Routing capability in CyberBOSS Server
  - Actions are directed to the domain where they are best suited
  - E.g., If federating a cyber range, a request to perform an attack should go there
- THIS IS A KEY CAPABILITY OFFERED BY THE SYSTEM
  - Routing between multiple domains, not just one.

CIF / CDM Description

- Cyber Data Model (CDM) provides common definition of cyber effects / events, objects and status
- CDM Javadoc / JSON documentation auto-generated at build-time for dynamic maintenance
- Approach allows us to evolve the model during research and integration efforts to incorporate new systems
- CyberBOSS Interface Framework (CIF) is a pre-built Java library that facilitates client use of the CDM.

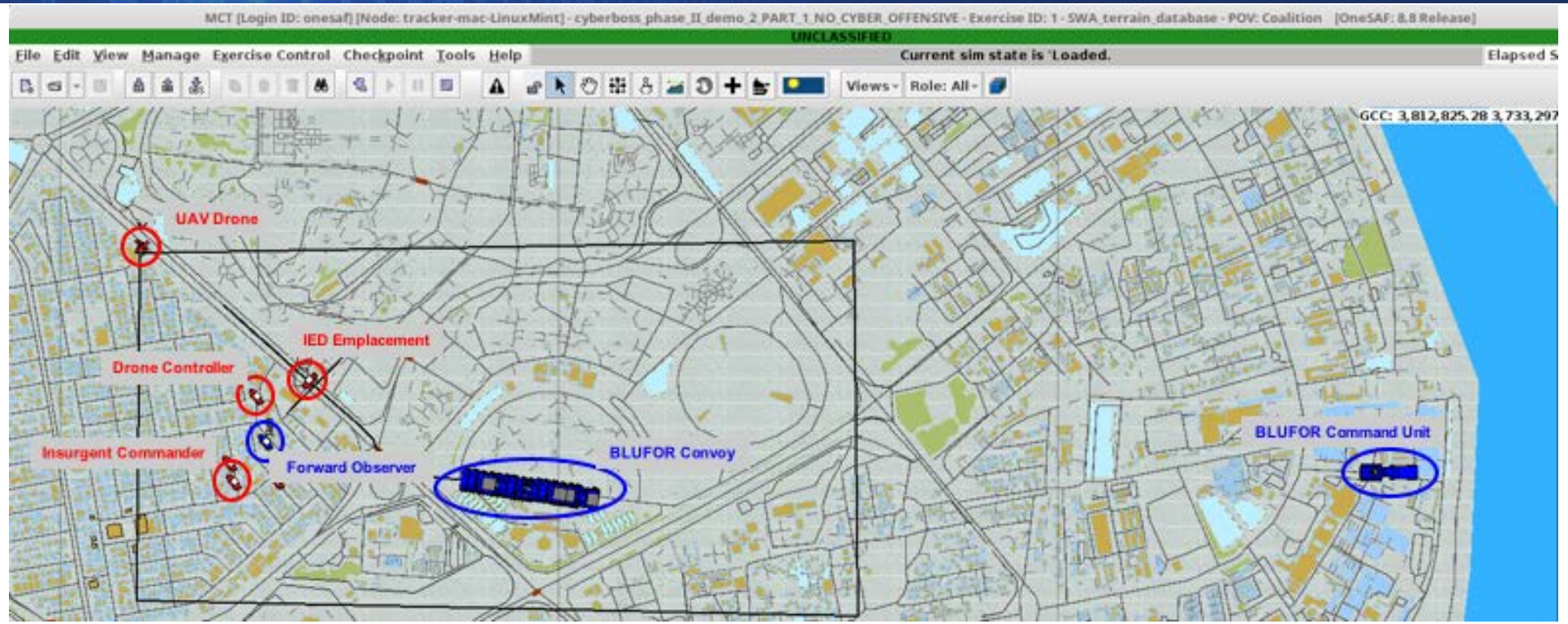



```
{
  "cdmType": "Device",
  "name": "ipsum",
  "id": "1cdb9898-f771-4a66-ab8d-65cdf5743300",
  "applicationIDToDeviceKindMap": {},
  "deviceCyberPropertiesMap": {},
  "deviceStatesMap": {},
  "deviceAttributeMap": {},
```

Demo Objectives

- Demonstrate flexible and configurable cyber training environment
  - E.g., Can opt to include a cyber range, or train without one, with minimal configuration
- Demonstrate cross-domain communication with CyberBOSS as a broker
  - Reconnaissance and attack operations interoperate over disparate applications (LVC & cyber range)
  - Demonstrate connections to cyber range
- Develop more complex scenarios that support offensive cyber training
- Exemplify how the Cyber Data Model (CDM) can be extended to support robust client integration
- Prototype the CIF as a standardized client API / connection paradigm
  - Extend OneSAF to show vision of how a compliant cyber simulation would interface with CyberBOSS
    - Utilize prototype CIF client adapter (within OneSAF)
    - Build ODM, Modeling & Agent Infrastructures (following OneSAF development paradigm)
- Demonstrate COBWebS REST API integration

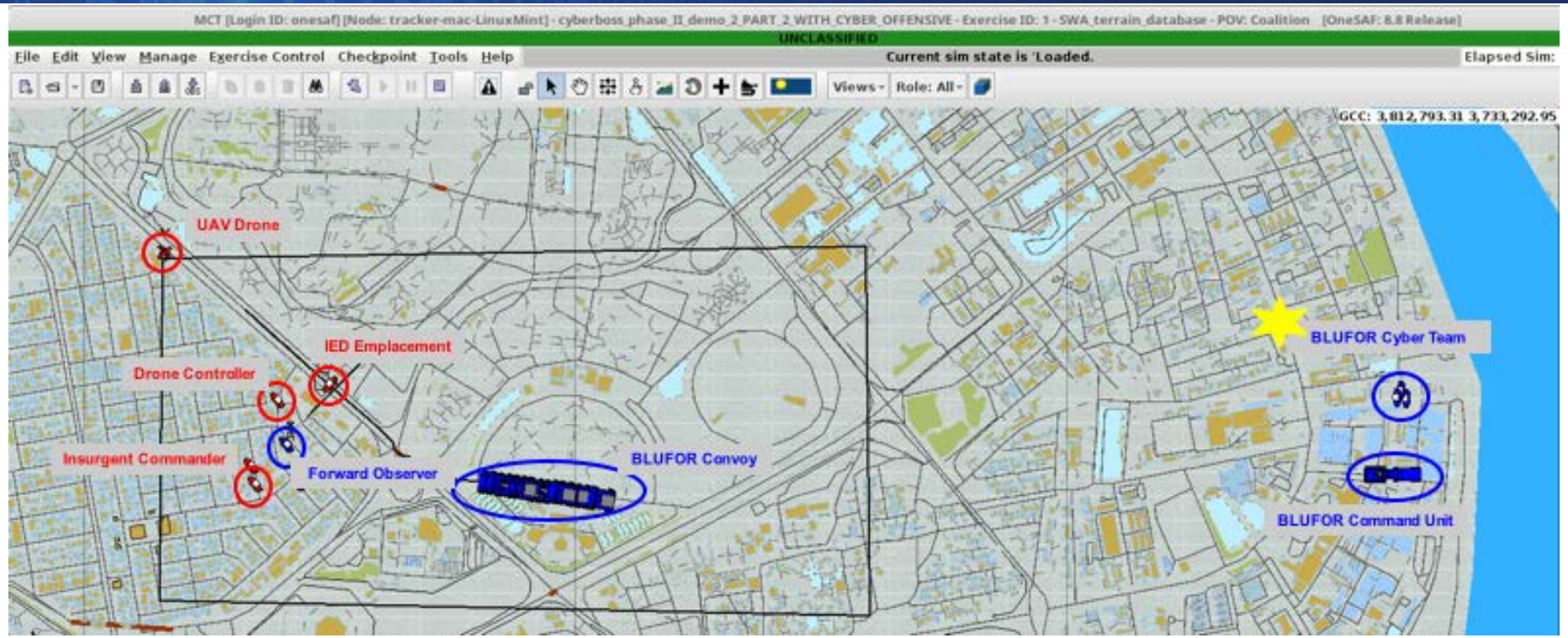
Demo Part 1: *NO* Cyber Offensive



- Part 1: *NO* BLUFOR Cyber Offensive
  - BLUFOR convoy traveling down route in urban environment
  - OPFOR insurgents situated in WiFi cafes, using a drone to surveil convoy activity
  - Commander instructs movement of convoy, unaware of insurgency coordinated IED attack
    - Denial of Service (DoS) on commander's tactical device
    - Demonstrates extension of COBWebS into more complex training scenarios
  - BLUFOR Forward Observer attempts to relay impending attack to commander, but message fails
  - Convoy moves through area, IED detonated with BLUFOR casualties

- KEY OBJECTIVES
  - Demonstrate ability to create OPFOR cyber attacks through COBWebS using the CyberBOSS Control Tool
  - Demonstrate modeling of OPFOR offensive cyber operations
  - Demonstrate cyber training capabilities when cyber range is unavailable

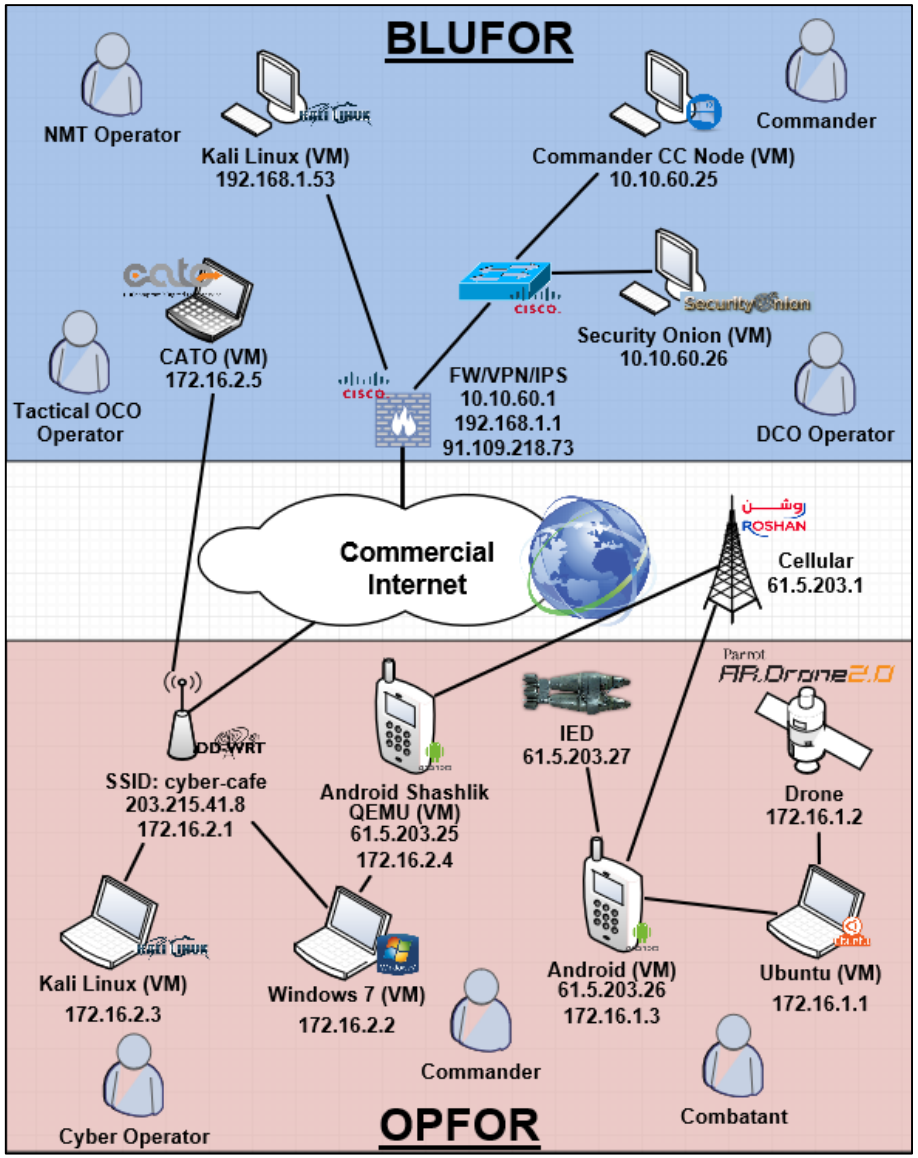
Demo Part 2: *WITH* Cyber Offensive



- Part 2: *WITH* BLUFOR Cyber Offensive
  - BLUFOR commander mitigates active attack on internal network by ordering cyber reconnaissance
    - Obtains ability to hack into OPFOR controlling devices for drone & IED detonator
  - BLUFOR commander orders cyber attack on the OPFOR devices
  - OPFOR loses communication with the UAV drone and can no longer surveil the BLUFOR convoy
  - OPFOR cannot initiate IED
  - BLUFOR convoy moves through the area unharmed.

- KEY OBJECTIVES
  - Demonstrate interoperability of cyber range and constructive simulation systems to provide cyber training
  - Demonstrate modeling of BLUFOR offensive cyber operations
  - Demonstrate collaborative training between Maneuver & Cyber Team

Demo Cyber Battlespace



U.S. ARMY RESEARCH, DEVELOPMENT AND ENGINEERING COMMAND

Cyber Warfare for Training Research (CyWar-T)

Nathan Vey

Science & Technology Manager

Simulation & Training Technology Center (STTC)

13 AUG 2018

APPROVED FOR PUBLIC RELEASE

WHY CYWAR-T?

Modernization Priorities for the United States Army

#2 An Army Network with Hardware, Software and Infrastructure

Combine cyber and kinetic domains through simulation to exploit and analyze implications of one domain on another.

#6 Soldier Lethality that Spans all Fundamentals

Representation of Cyber and Electromagnetic Activities (CEMA) in simulated Operational Environments.

Army Modeling and Simulation Office (AMSO)

- Cyber / Electronic Warfare (EW) Working Group
- Prioritized, Refined Gaps from all Modeling & Simulation Communities

---

Project Manager for Constructive Simulation (PM ConSim)

- Cyber listed as #1 technology gap

CYBER WARFARE PROTOTYPE

Develop a loosely coupled software service that models the effects of Cyber- and Electromagnetic-attacks on Blue (friendly) mission command devices. Initial focus on “Cyber for Others” training.

- Modeled attacks include:
  - Denial of Service (DoS)
  - Information Interception (II)
  - Information Forgery (IF)
  - Information Delay (ID)

Technologies Used:

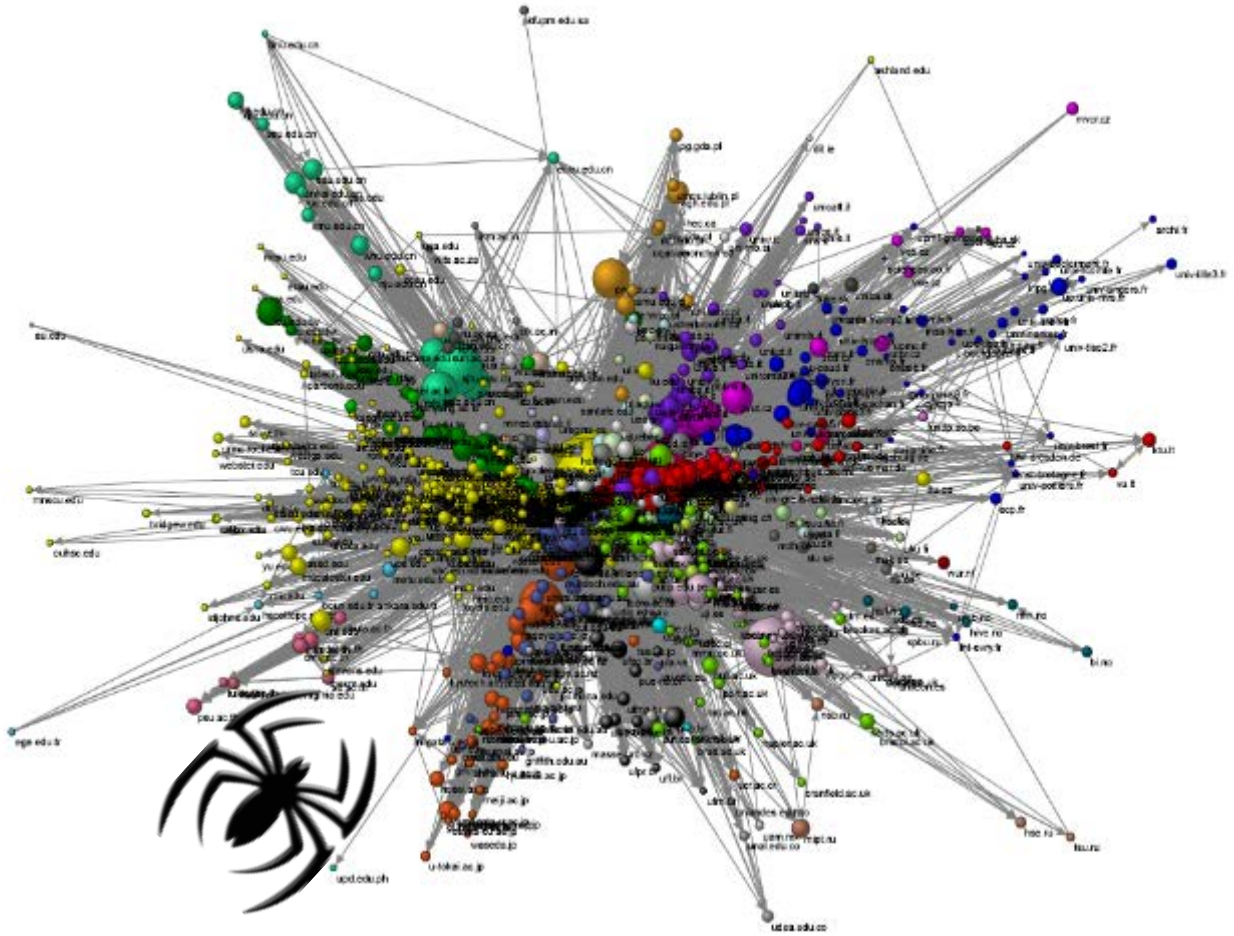
- Leverage Mission Command Adapter Web Service (MCA-WS) plugin from the One Semi-Automated Forces (OneSAF) program to simulate the effects of cyber attacks on mission command devices
- Must keep Information Assurance requirements of simulation system

Provide a foundational capability that can be used on a wide range of training use cases.

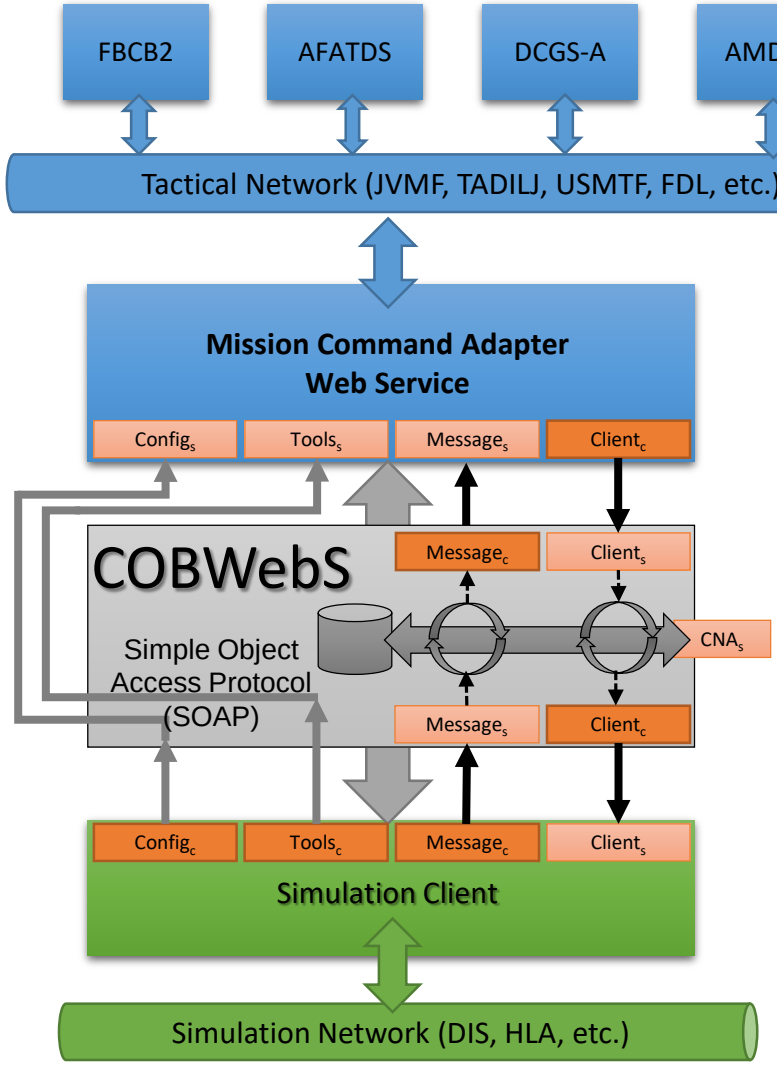
PROTOTYPE DESIGN

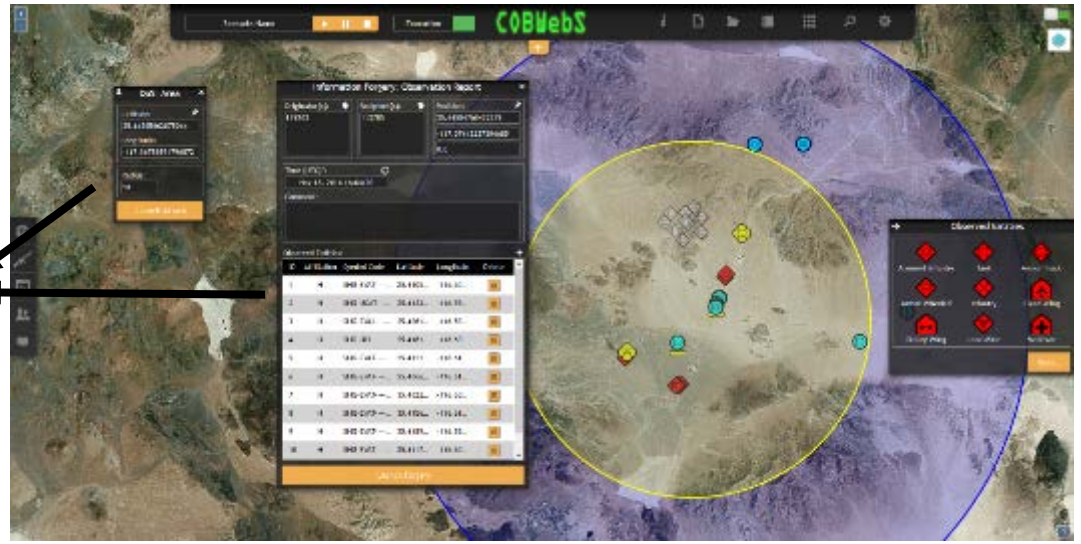
COBWebS

Cyber
Operations
Battlefield
Web
Service



COBWEBS OVERVIEW





LEGEND

<SERVICE NAME>$_c$ — Web service – client side

<SERVICE NAME>$_s$ — Web service – server side

Note : Unit Reference Numbers (URNs) are Fictional

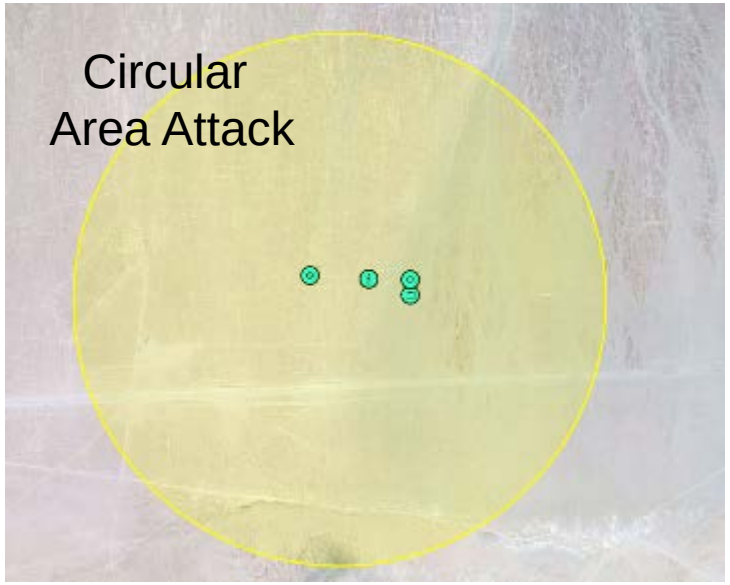
COBWEBS CAPABILITIES

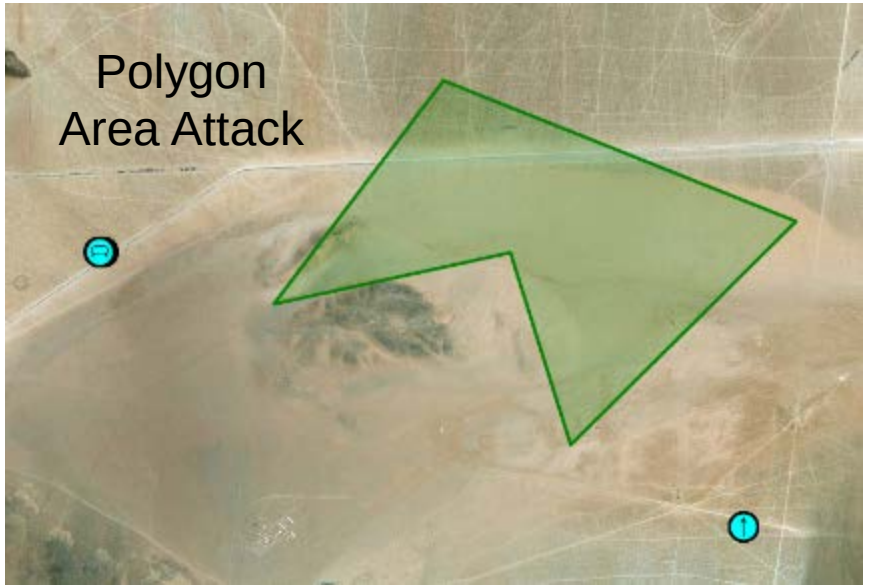
- **Incorporates cyber warfare elements into exercises to meet training objectives.**
  - Creates cyber effects of attacks such as electronic warfare, kinetic and hacking. Scenario developers can define the storyline.
  - Allows trainees to experience symptoms of cyber attacks.
  - Leaders can develop contingencies, based on what has been compromised.
    - Workarounds
    - Alternative Courses of Action (COAs)
    - Procedures based on detecting, responding to, and recovering from a cyber attack.

- **Provides an Information Assurance (IA) safe environment without corrupting the network infrastructure.**
  - Typical in cyber range exercises
  - Can be integrated with cyber test ranges

- **Software only solution – no special hardware required.**

CYBER ATTACK EDITOR



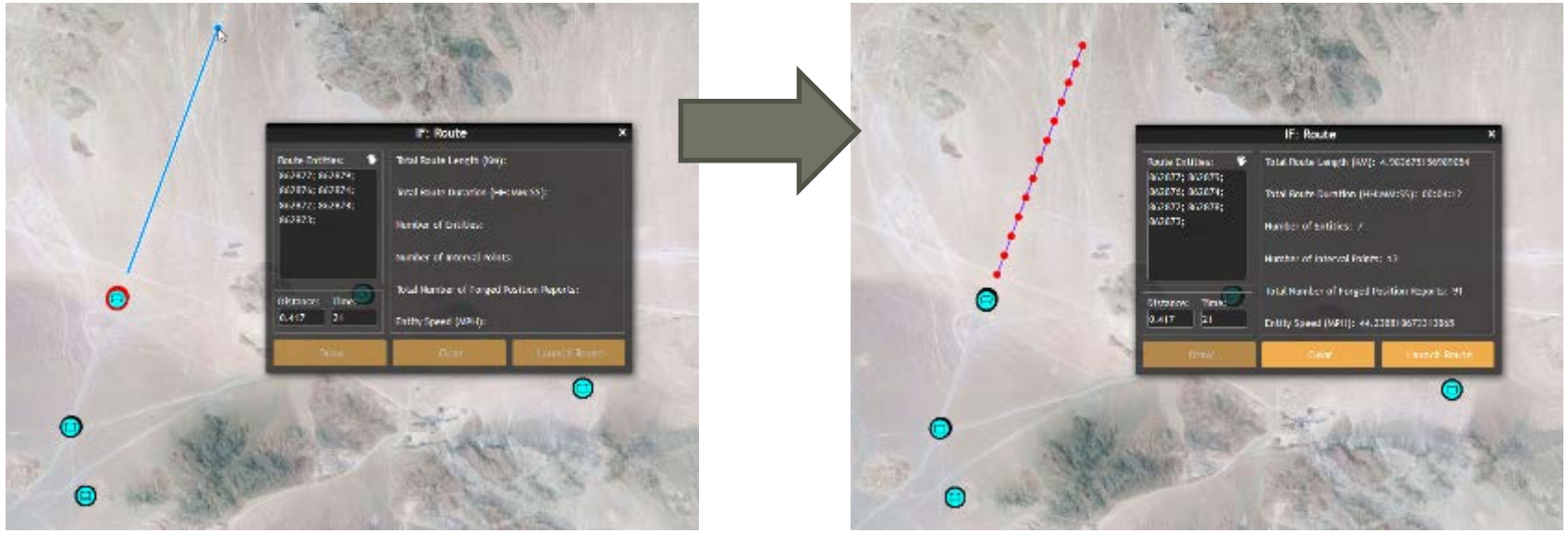


The map is fully interactive and supports Area based Attacks (Circular and Polygon) and URN based Attacks.

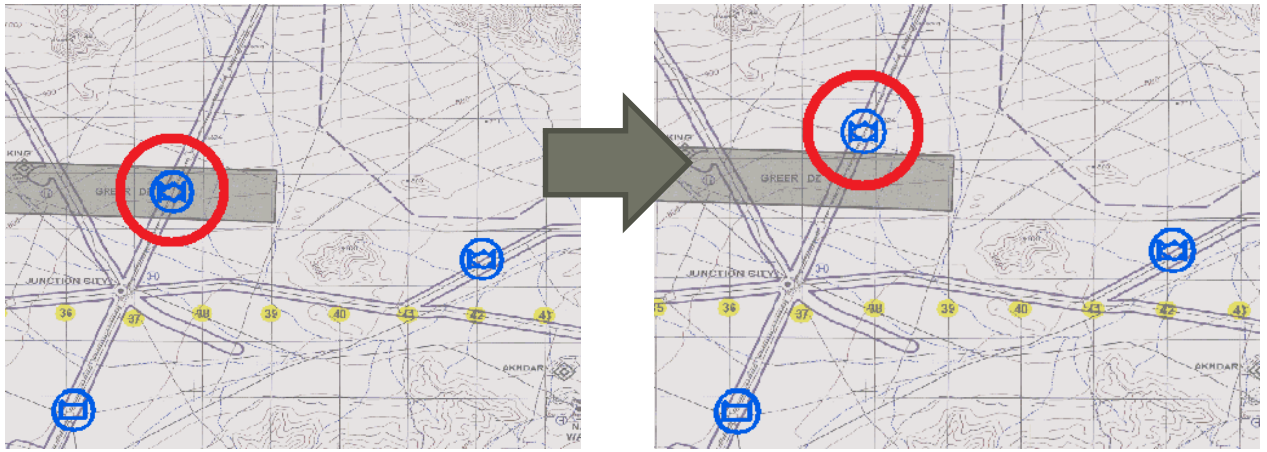
Map supports online and offline terrain tiles.

URN = Unit Reference Number

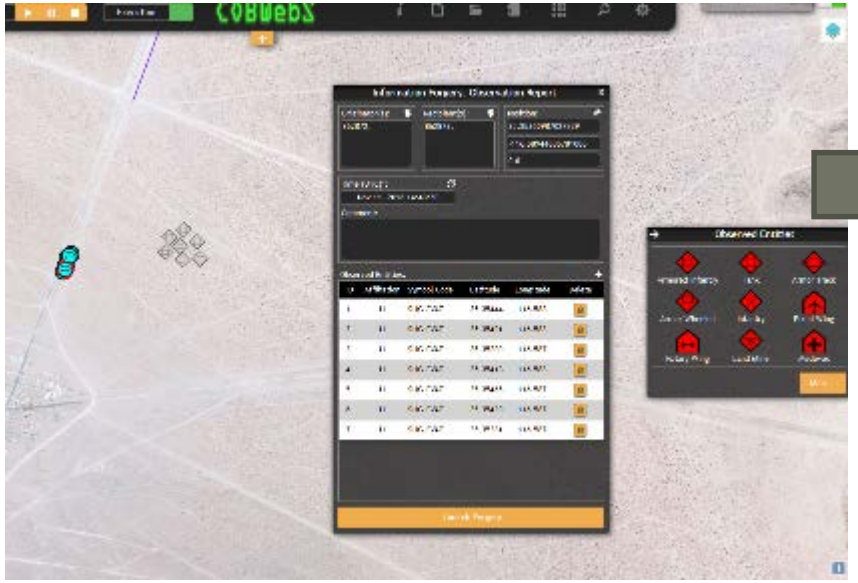
CYBER ATTACK EDITOR – FORGED POSITION REPORT

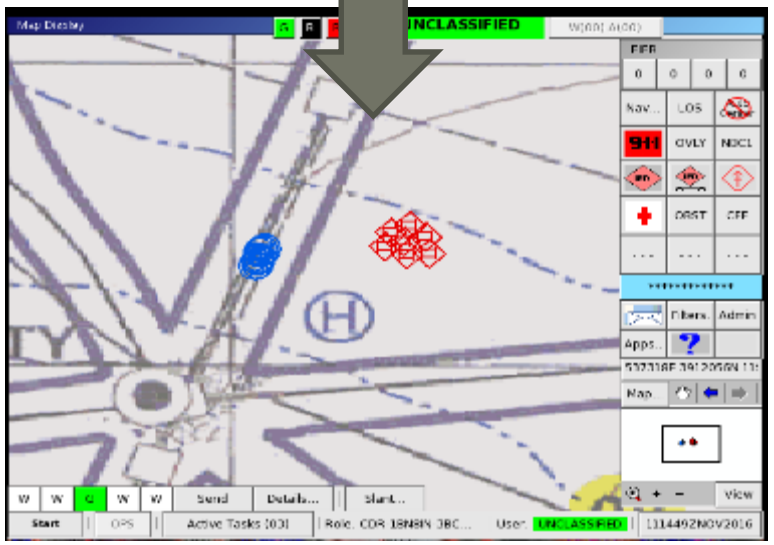


Allows forged information like Position Reports, routes, Spot Reports, and text messages to mislead Blue Forces (BLUFOR)



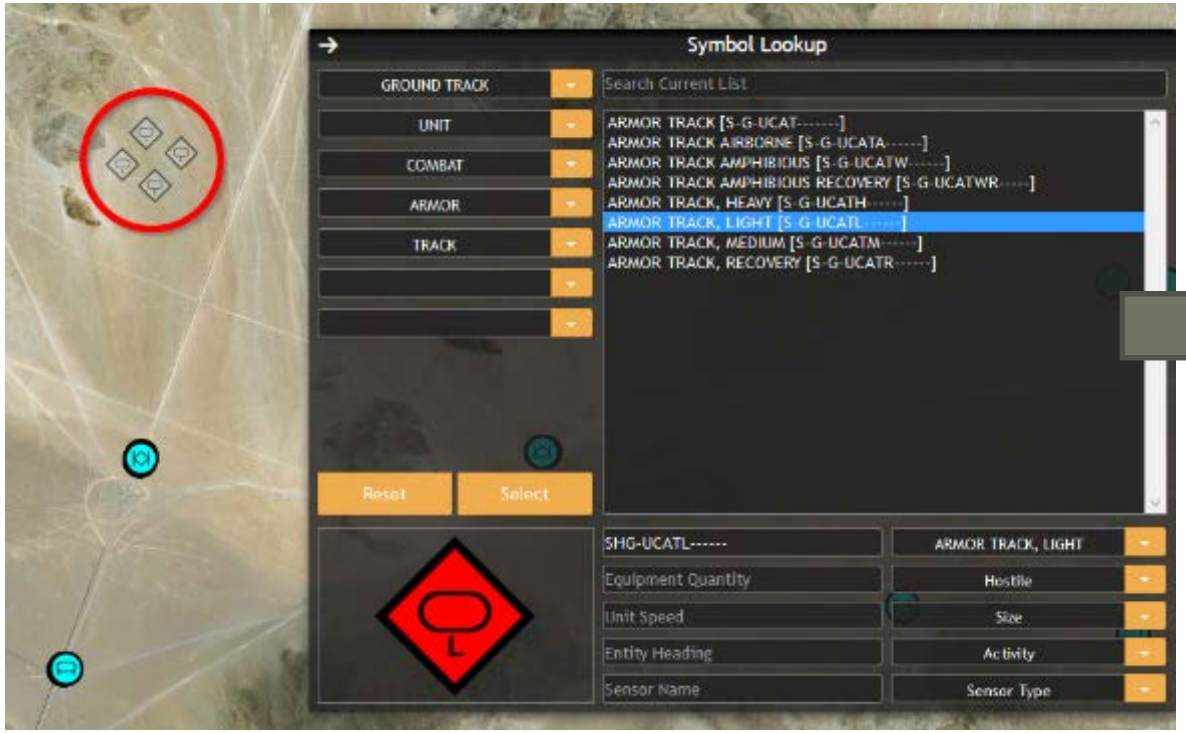
CYBER ATTACK EDITOR – FORGED SPOT REPORT

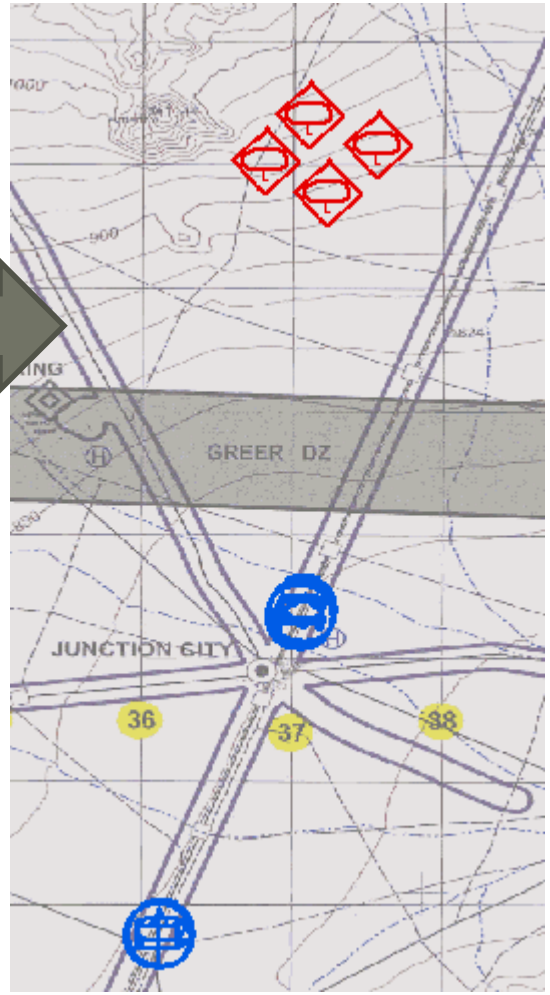




Example Spot Report forgery to distract BLUFOR.

CYBER ATTACK EDITOR – FORGED SYMBOL LOOKUP



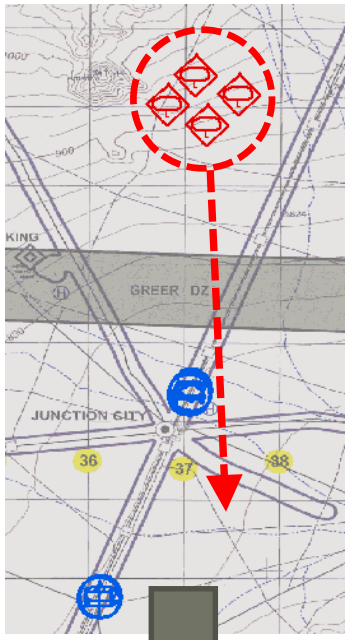


Cyber Attacker Role Player has ability to forge any symbol using Symbol Lookup feature.

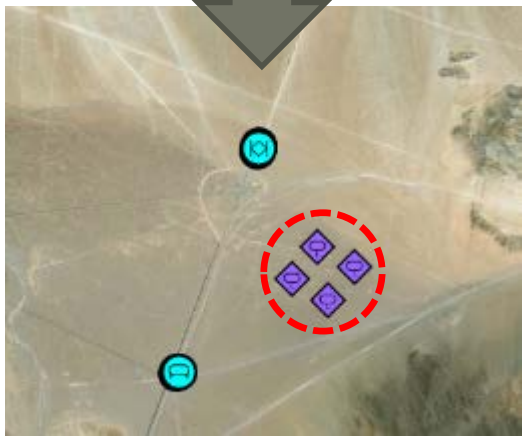
CYBER ATTACK EDITOR – MOVING FORGERIES

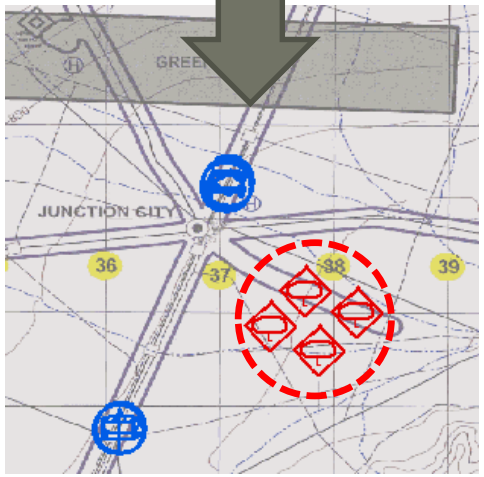
Cyber Attacker can **move** forgeries in Cyber Editor and updates are reflected on tactical devices.

Before Move

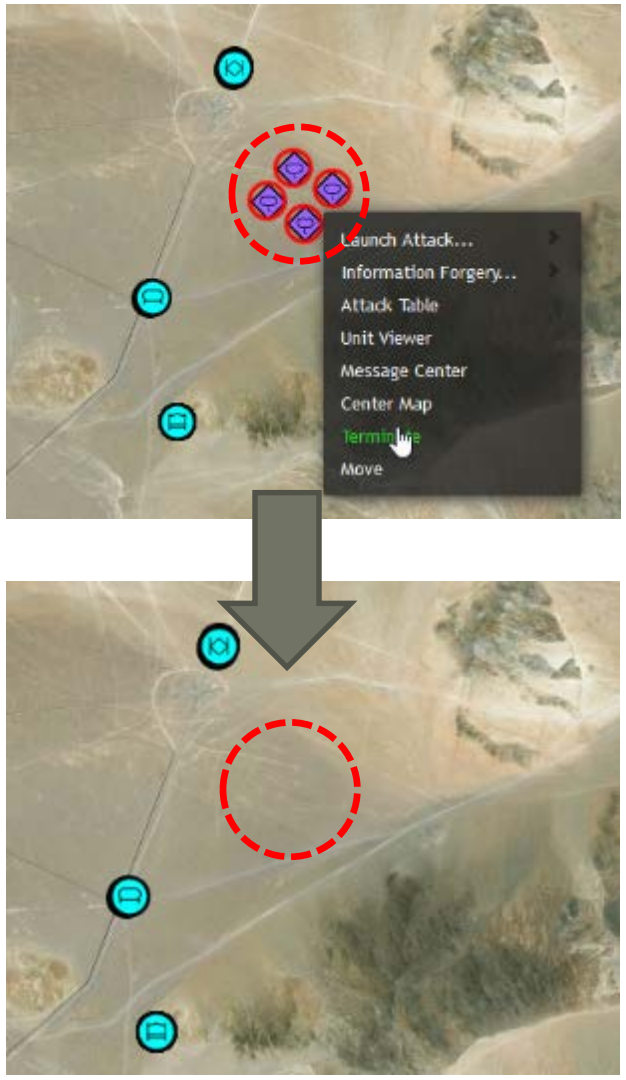


After Move





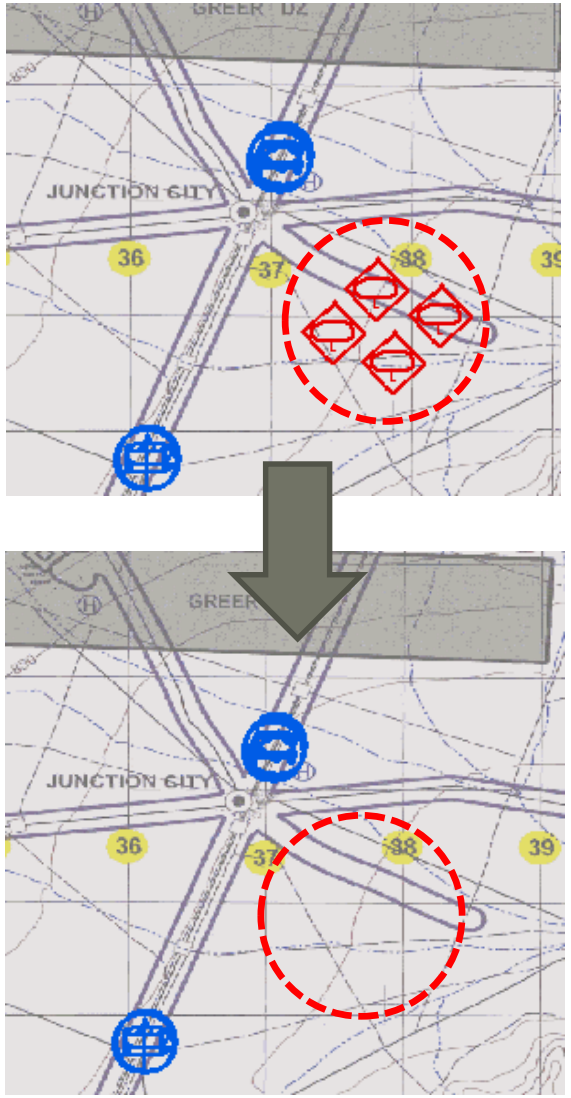
CYBER ATTACK EDITOR – TERMINATE FORGERIES



Cyber Attacker can **terminate** forgeries in Cyber Editor and symbols are removed from tactical devices.

Before Terminate

After Terminate



MISSION MANAGER

- Mission Manager allows cyber exercises to be created and saved
- Can save single missions or scenarios (multiple missions)

MISSION MANAGER – TIME TRIGGERS

Time Triggers

Cyber Attacks will automatically launch at specified Mission time.

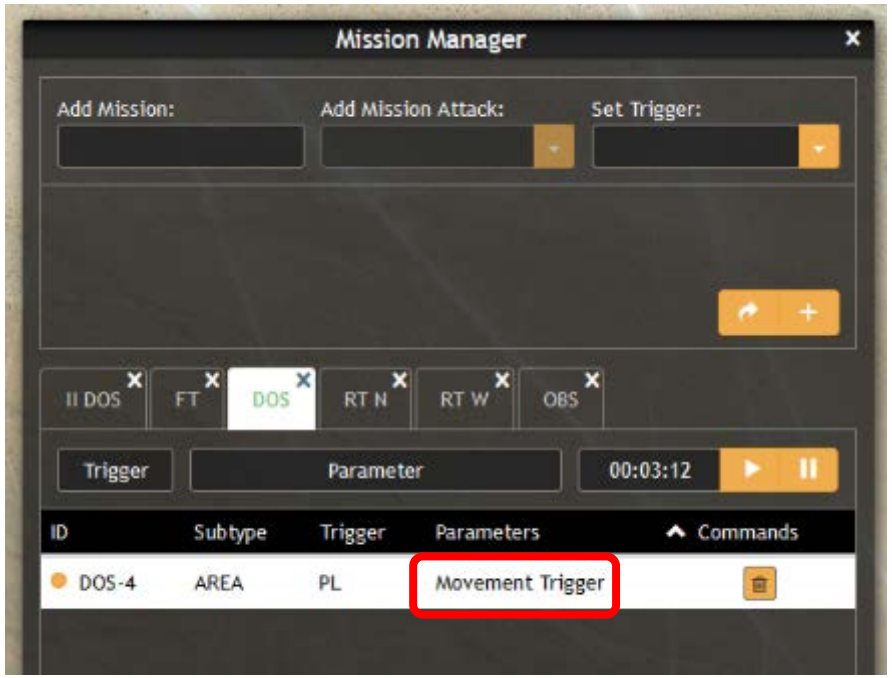
Example:

Free Text Message forgeries will launch at Mission time 00:00:00 and Mission time 00:00:05.

MISSION MANAGER – PHASE LINE TRIGGERS

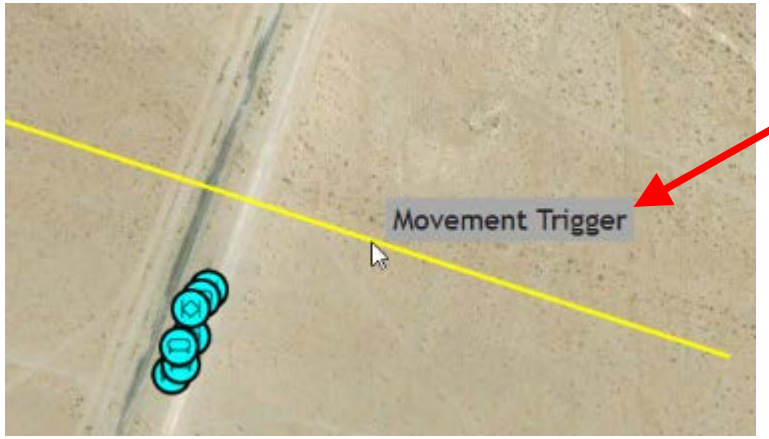
Phase Line Triggers

Cyber Attacks will automatically launch when any of the specified entities cross the designated phase line.



Example:

Denial of Service (DoS) Attack will launch when entities cross yellow phase line.



MISSION MANAGER – COMPLETION TRIGGERS

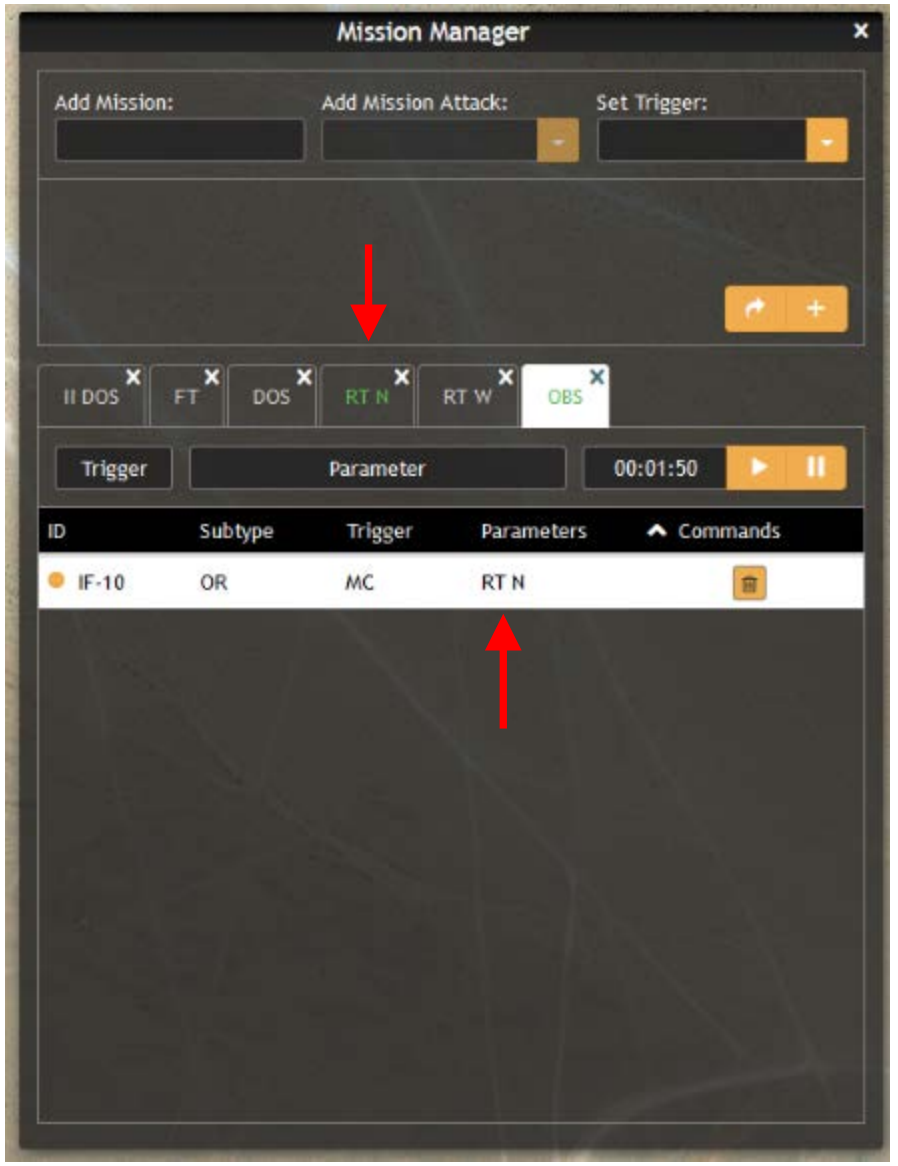
Completion Triggers

Cyber Attacks will automatically launch when the specified Mission or Mission Attack is completed.

This gives the Cyber Attacker Role Player the ability to daisy chain Cyber Attacks.

Example:

Observation Report Forgery Attack will launch when RT N Mission completes.



CONCLUSION

- On-going research that explores methods to create cyber and electromagnetic effects in current Live, Virtual, and Constructive (LVC) training systems.
- COBWebS is designed to provide Cyber Simulation Effects in current training simulations, producing Cyber operation attack effects like information delay, forgery, interception, and denial of service in Mission Command Systems. Uses current simulation components like the Mission Command Adapter Web Service (MCA-WS) to produce effects.
- COBWebS version was transitioned to One Semi-Automated Forces (OneSAF) version 8.8 (AUG 2018 release).
- Transition Agreement (TA) with PEO STRI.
- Phase II Small Business Innovation Research (SBIR) to develop a data exchange model to connect stimulate cyber effects in multiple connected simulation systems from a live cyber range.
- Two Phase I SBIRs seeking to add a cyber-intelligent Opposing Force (OPFOR) into current training simulation systems.
- Two AMSO efforts to address gaps identified by Cyber / Electronic Warfare (EW) Working Group: 1) Simulate Cyber/EW Effects in Mission Command Information Systems & 2) Modular Modeling and CEMA Framework.

NTSA
I/ITSEC 2018
NOV 26TH – Nov 30TH | ORLANDO, FL
LAUNCHING INNOVATION IN LEARNING:
READY, SET, DISRUPT

iSCORE Overview

Intelligent Simulated Cyber OPFOR Reactive Engine

Phase I Army SBIR

Lloyd Wihl, Jeff Weaver, Rajive Bagrodia, Chris Hawkins

SCALABLE Company Overview

What We Do

- Deliver network virtualization technology for **development, analysis, test and cyber assessment & training for applications & networks** to military, governmental, commercial, and educational institutions around the world
- Enable users to **EVALUATE the effectiveness and cyber resiliency of networked communications environments**, and **TRAIN** the users of large net-centric systems over the life of the environment

Core Technologies

Network Simulation

- High-fidelity, real-time simulation platform
- Detailed protocols/waveforms (MANET, LTE, Wi-Fi, SATCOM, sensor, tactical battlefield protocols, etc.
- Emulation interfaces for L-V-C integration

Cyber Behavior Models

- Simulated cyber attack, defense & vulnerability models: Jamming, DoS, IPSec, PKI, Eavesdropping, SIGINT, Rootkit, Botnet,
- Host Model with vulnerability framework and configurable exploit actions

Key Clients And Markets Served

Defense | Industry | Government

US Army, US Air Force, US Navy, CERDEC

APL, AT&T, Boeing, CAE, EADS, France Telecom, GE, General Dynamics, Google, Honeywell, L3, Lockheed Martin, Lucent Technologies, Microsoft, Mitsubishi Electric, MITRE, NASA, NIST, Northrop Grumman, NTT DoCoMo, Panasonic, Parsons, RAND, Raytheon, SPAWAR, Thales, Toshiba, Toyota

Key Discriminators

- Accurate real-time network emulation
- Leverage parallel model execution for scalability
- Comprehensive wireless and cyber attack & defense models

Overview

- iSCORE is a Phase I Army SBIR under the US Army's Natick Soldier Research, Development, & Engineering Center (NSRDEC) Simulation & Training Technology Center (STTC).

- iSCORE will allow for the automation of intelligent simulated OPFOR cyberspace attacks which can be integrated within multiple cyber test and training environments.

- iSCORE could potentially be used with multiple GOTS and COTS training environments that include OneSAF, CyberTASE (Cyber Test Analysis and Simulation Environment) Constructive Component (CCS), Network Defense Trainer (NDT) and others.

Impact of iSCORE

- Integrates cyber warfare into the Army's LVC&G kinetic training systems. Cyber and kinetic domains will affect each other.

- BLUFOR trainees will have the ability to recognize and react to cyber-attacks, defend the network and launch offensive cyber-attacks.

- Reduces the need for live red teams, reducing training costs, improving training scheduling, and enabling increased training "reps."

Replicate Red Team Strategies

The attack and attack vector models could initially be based upon an open source database, such as CVE/CWE.

The attacks consist of chains of actions that use triggers, where the triggers contain feedback from one attack that becomes the input for the next attack. For example:

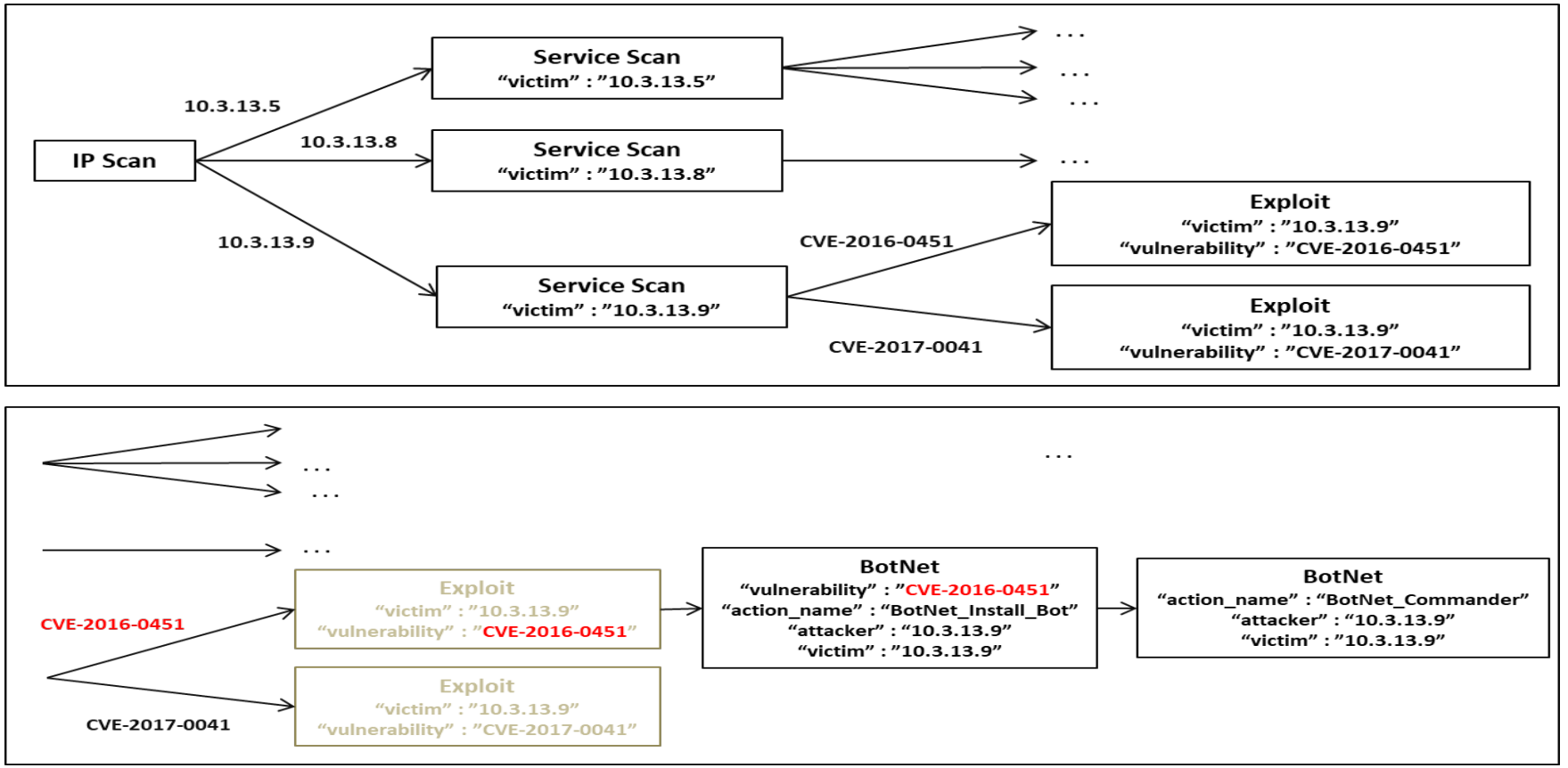
- Scan a network
- For each discovered IP address, scan its system services
- From discovered system services, derive vulnerabilities
- Exploit selected vulnerabilities

The exploits that are selected depend on their impact, so an impact model would be needed.

Outputs from the actions above would include:

- Discovered IP addresses
- Discovered system services and associated vulnerabilities
- Attack result (success, failure, timeout)
- Updated list of exploited victims

Replicate Red Team Strategies

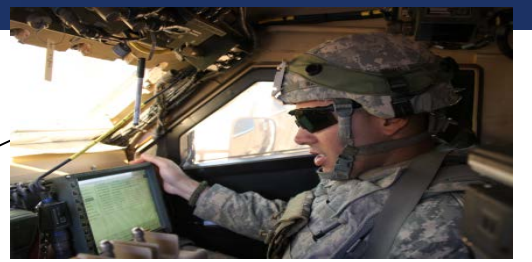


- Each vulnerability is examined to determine if its CIA impact and other attributes may imply its exploitation resulting in possible malware installation on compromised nodes, and from there attacking other nodes.
- Propagation of attacks through the network is achieved by sequences where compromised nodes become attackers.

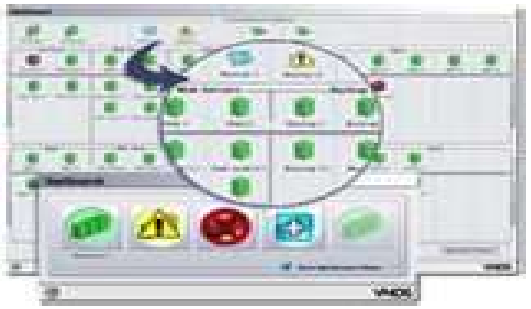
iSCORE Operational Concept

Network probes, impact models, intelligence, exploits, man-in-the-middle, adaptive attacks, defenses, …

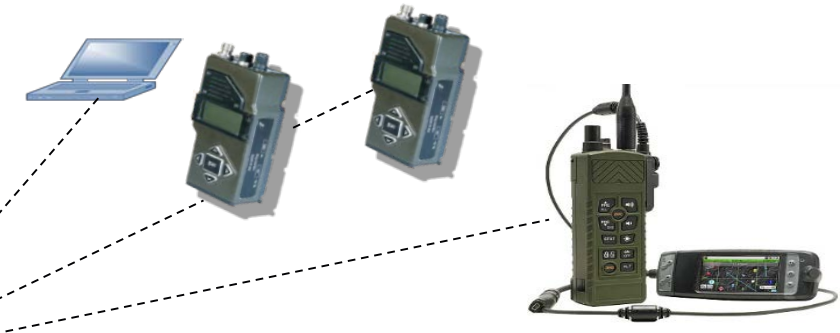
Constructive entity behavior



Adversary/friendly role players: commanders, staffs, network administrators

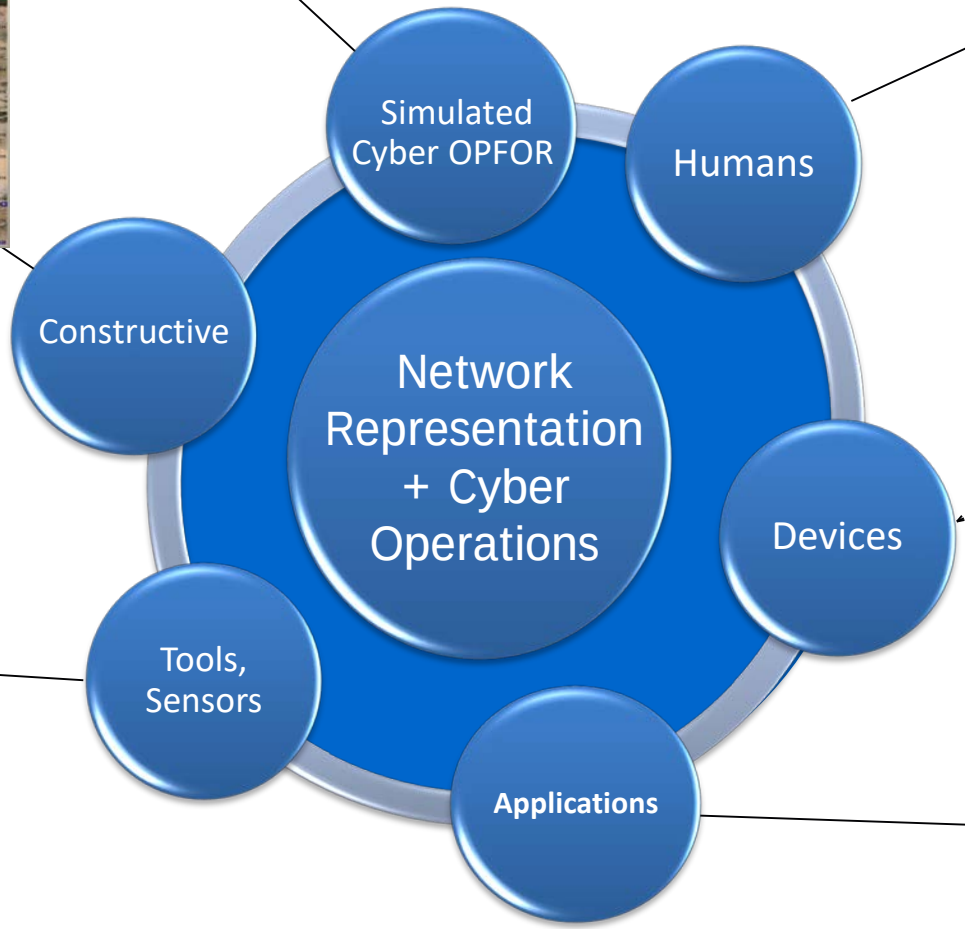


Manage network with standard network management / analysis tools, intrusion detection, firewalls, …



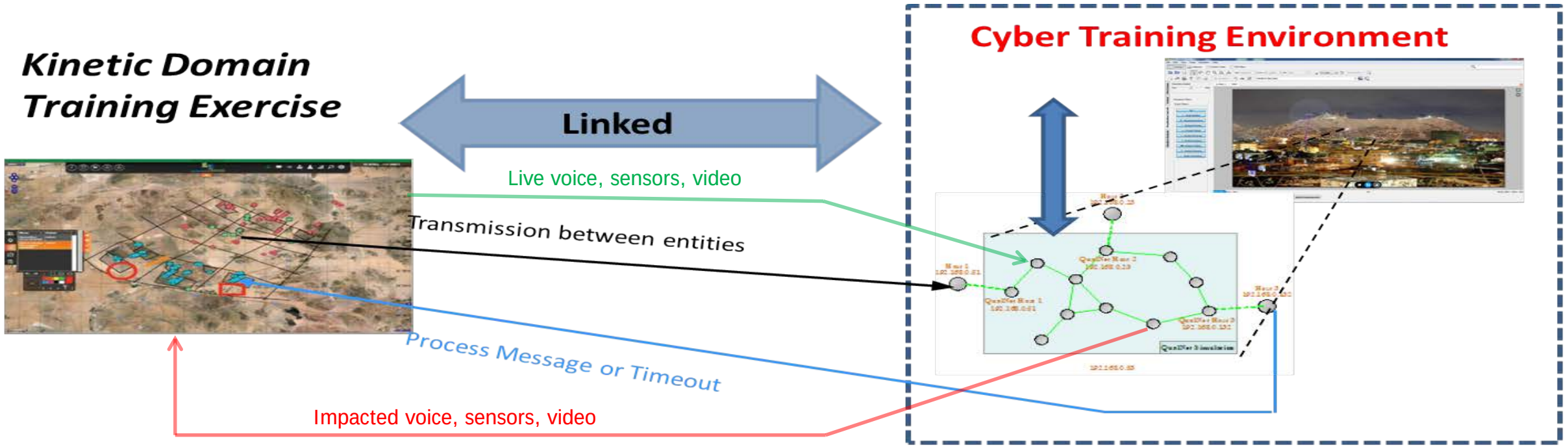
Connect live devices and networks to emulated network

Connect actual applications: control, video reconnaissance, etc.



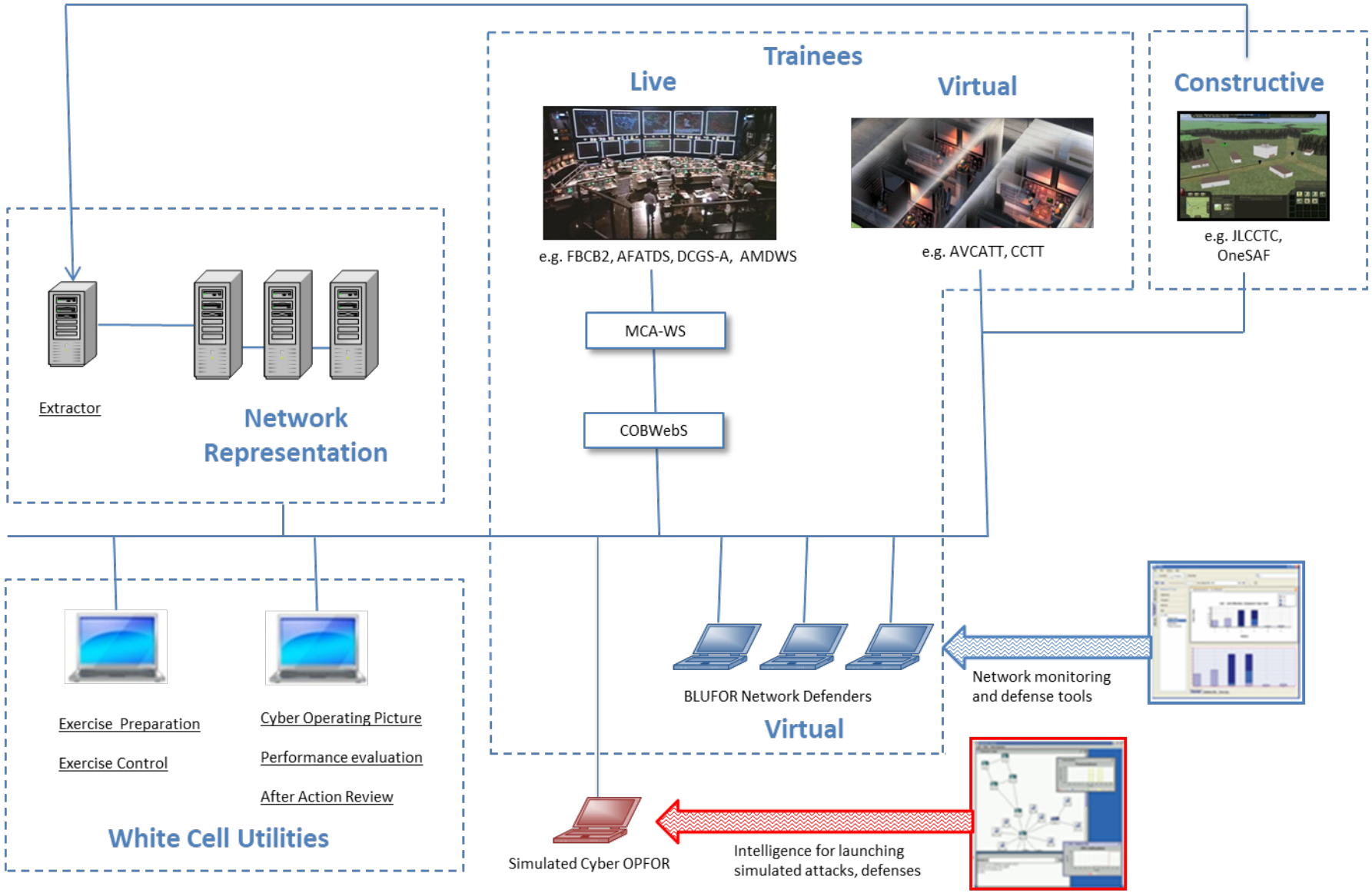
iSCORE Will Enable Cyber for Others Training

Introduces Cyberspace Operations Effects on Mission



- Kinetic and non-kinetic effects in the same space
- Integrated Live Virtual Constructive + cyber training
- Work through degraded cyber environment

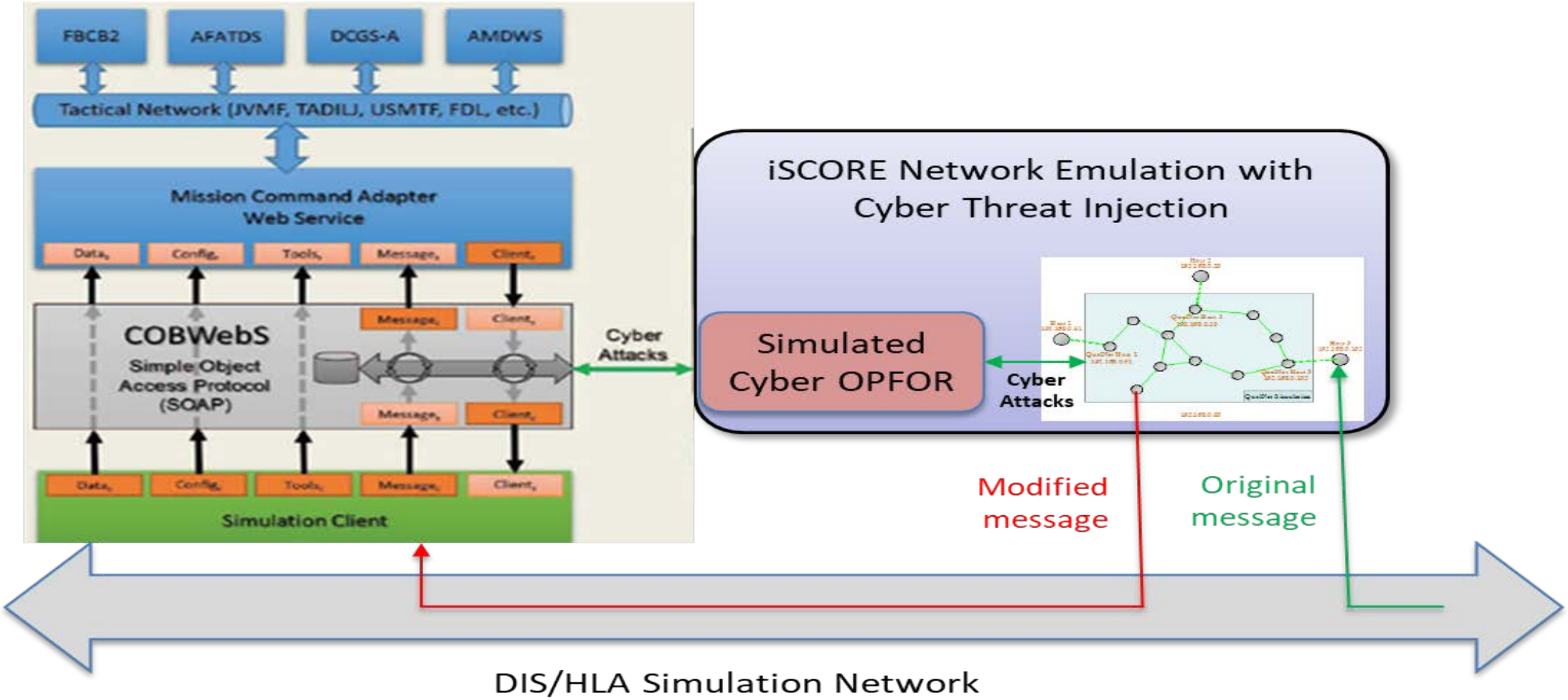
Example of a Potential Training System Deployment



Benefits of the iSCORE Concept

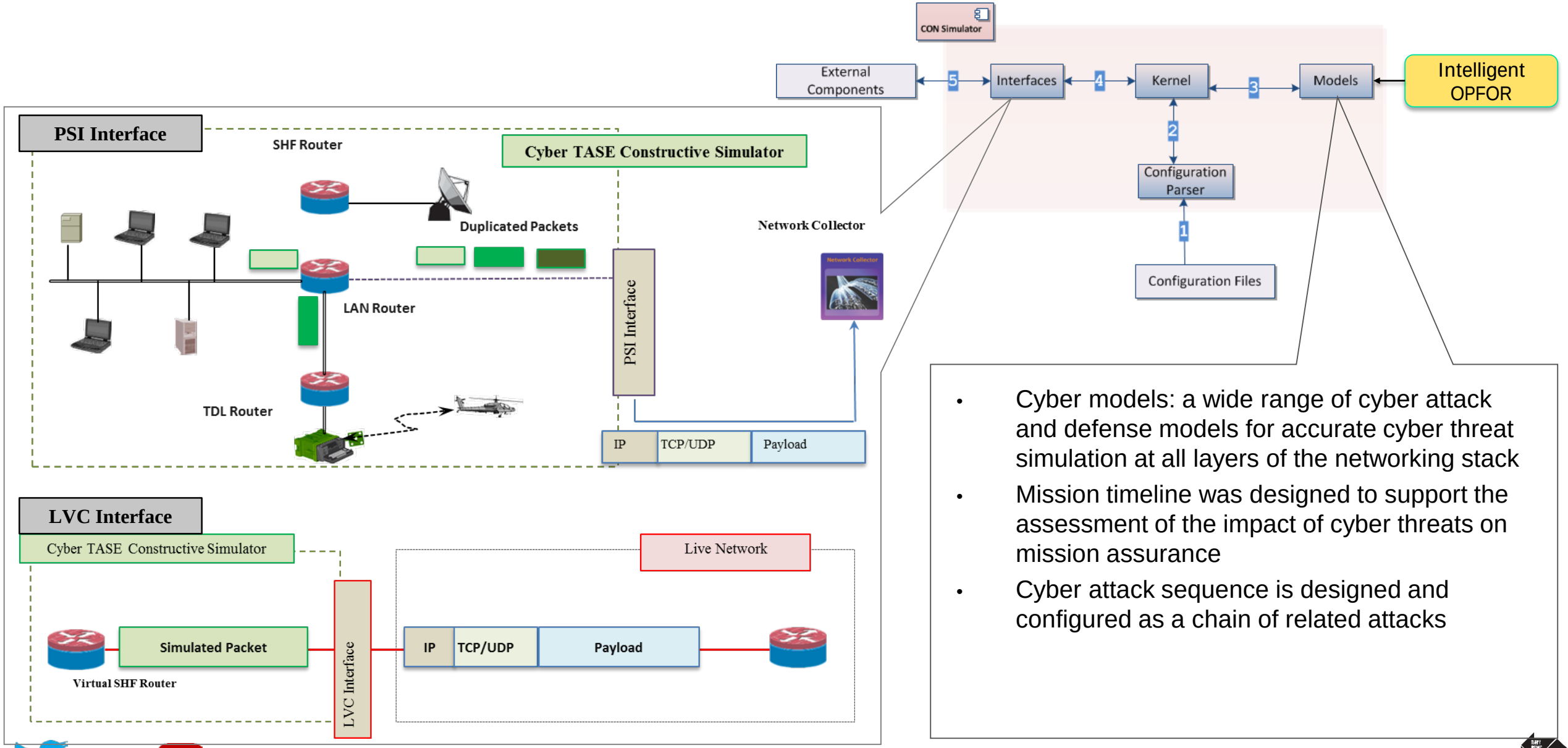
- **Safety**: Attacks are launched against virtual nodes in the software model of the network, and not against live systems. By mapping live systems to these virtual nodes, the effects of the cyber operations can be realized without compromising real systems.
- **Realism**: Accurate modeling provides responses to real attacks and defenses within a high-fidelity emulation environment. Can train blue cyber protection team.
- **Improvement over effects-based simulations**: Trainees can defend the network and launch cyber counterattacks. The emulated network responds to cyber defenses such as changes to firewall rules. Trainees can detect and work around data manipulation.
- **Improvement over IO PDU**: Simulations do not need to be updated to implement the effects of cyber-attacks. The network itself can be attacked.
- **Rich set of combat system threats**: jamming, eavesdropping, adaptive attacks, and host models with simulated vulnerabilities and exploitations that allow the incorporation of zero-day vulnerabilities in an exercise.
- **Readily integrated into Army training exercises**. Can inject cyber-attacks among all LVC&G participants. The architecture can also support affecting live-to-live communications, if desired.
- **Does not require MCA-WS** (but could work with it). Can work in conjunction with COBWebS.
- **Leverages existing interface** with-OneSAF. The OPFOR cyber intelligence will build on existing adaptive attack script functionality.
- **Both BLUFOR and OPFOR assets and networks** can be modeled, attacked and defended, combining kinetic and cyber warfare, with damage in one domain affecting performance in the other.

Example: Integration with COBWebS



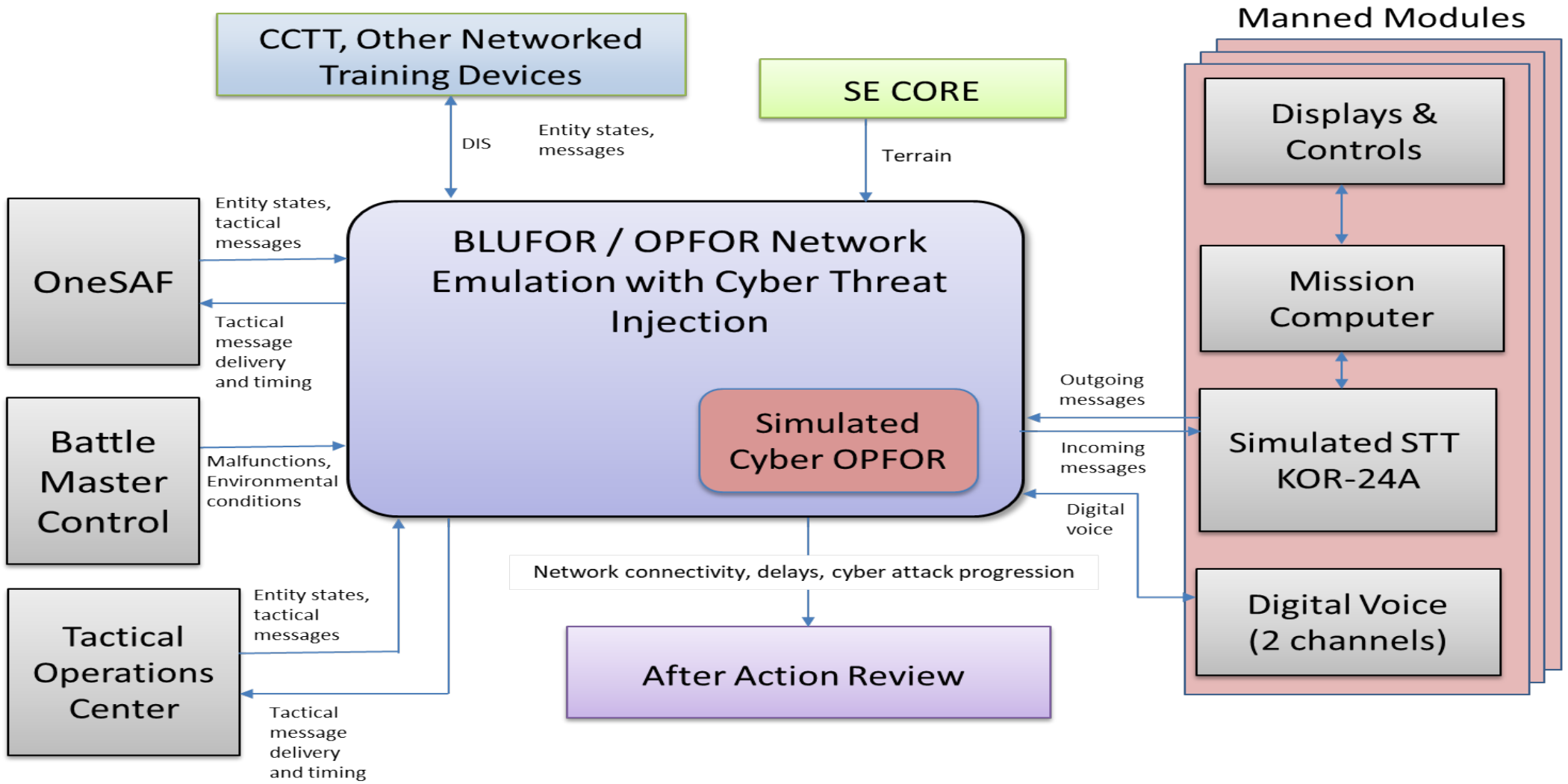
iSCORE Simulated Cyber OPFOR Integration with COBWebS

Example: Integration with CCS



- Cyber models: a wide range of cyber attack and defense models for accurate cyber threat simulation at all layers of the networking stack
- Mission timeline was designed to support the assessment of the impact of cyber threats on mission assurance
- Cyber attack sequence is designed and configured as a chain of related attacks

Example: Integration into AVCATT



Technology Transition Path

- Commercialize iSCORE as a robustly-packaged third party interface that can be used to connect a variety of existing trainers used by the Army to support automated injection of cyber effects.
- Integrate iSCORE as an add-on component to currently used GOTS network & cyber M&S framework JNE / StealthNet to serve as an intelligent simulated cyber OPFOR capability.
- Eventually propose a Phase 3 effort to use JNE-iSCORE to deliver advanced integrated cyber-and-kinetic training and analysis services to a diverse set of users from the Army and other services.

THANK YOU

Scalable Network Technologies, Inc.

6059 Bristol Parkway
Suite 200
Culver City, CA 90230

+1.310.338.3318 tel

info@scalable-networks.com

scalable-networks.com

iSCORE Govt. POC:

Nathan Vey
STTC / NSRDEC
nathan.l.vey.civ@mail.mil

C2SIM in CWIX

Distributed Development and Testing for Multinational Interoperability

Dr. Mark Pullen
George Mason University C4I & Cyber Center, USA

Lionel Khimeche
DGA, France

Kevin Galvin
Thales, UK

Introduction to C2-Simulation Interoperation

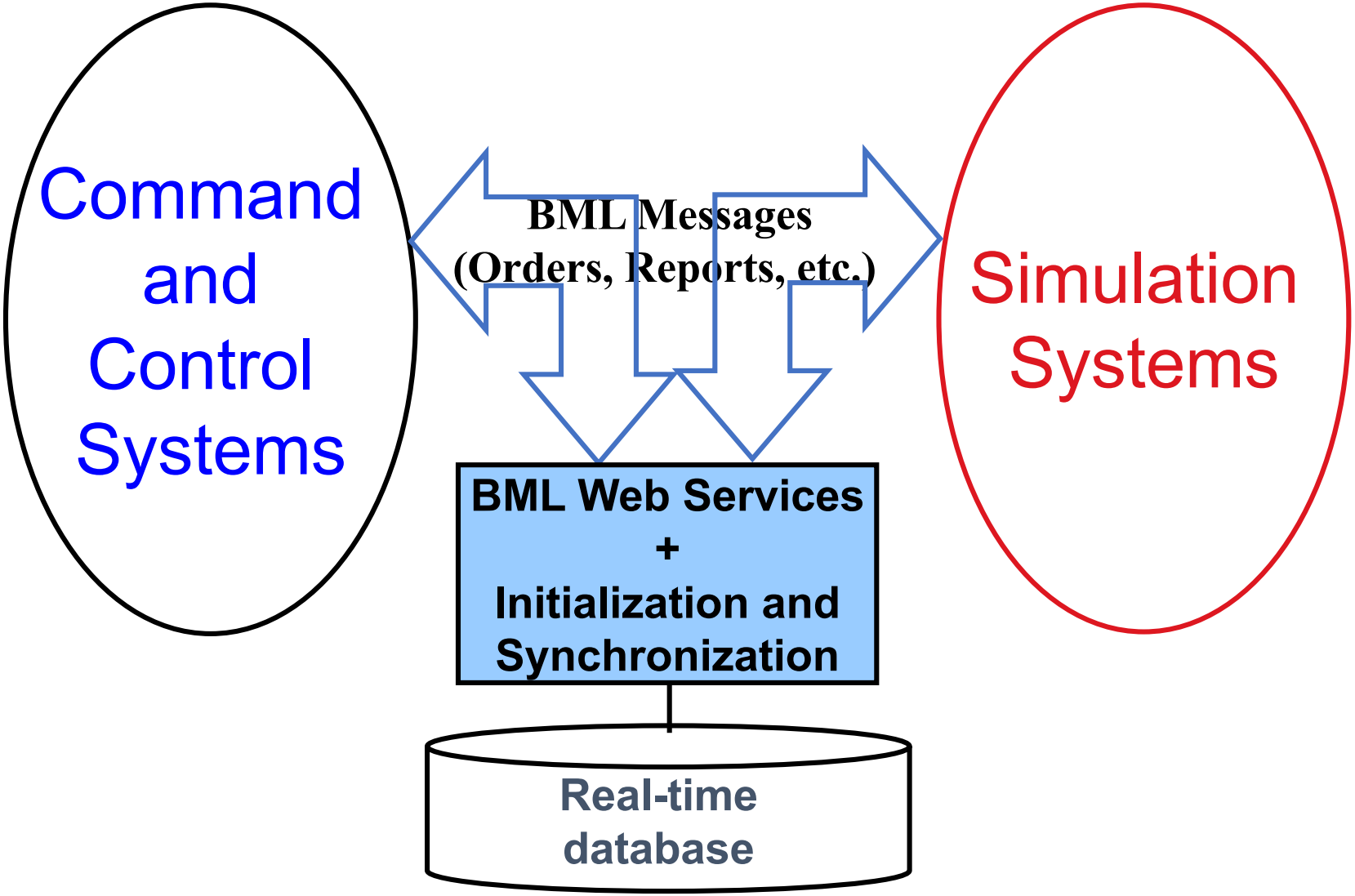
C2SIM Vision

We are working toward a day when the members of a coalition interconnect their networks, command and control (C2) systems, and simulations simply by turning them on and authenticating, in a standards-based environment.

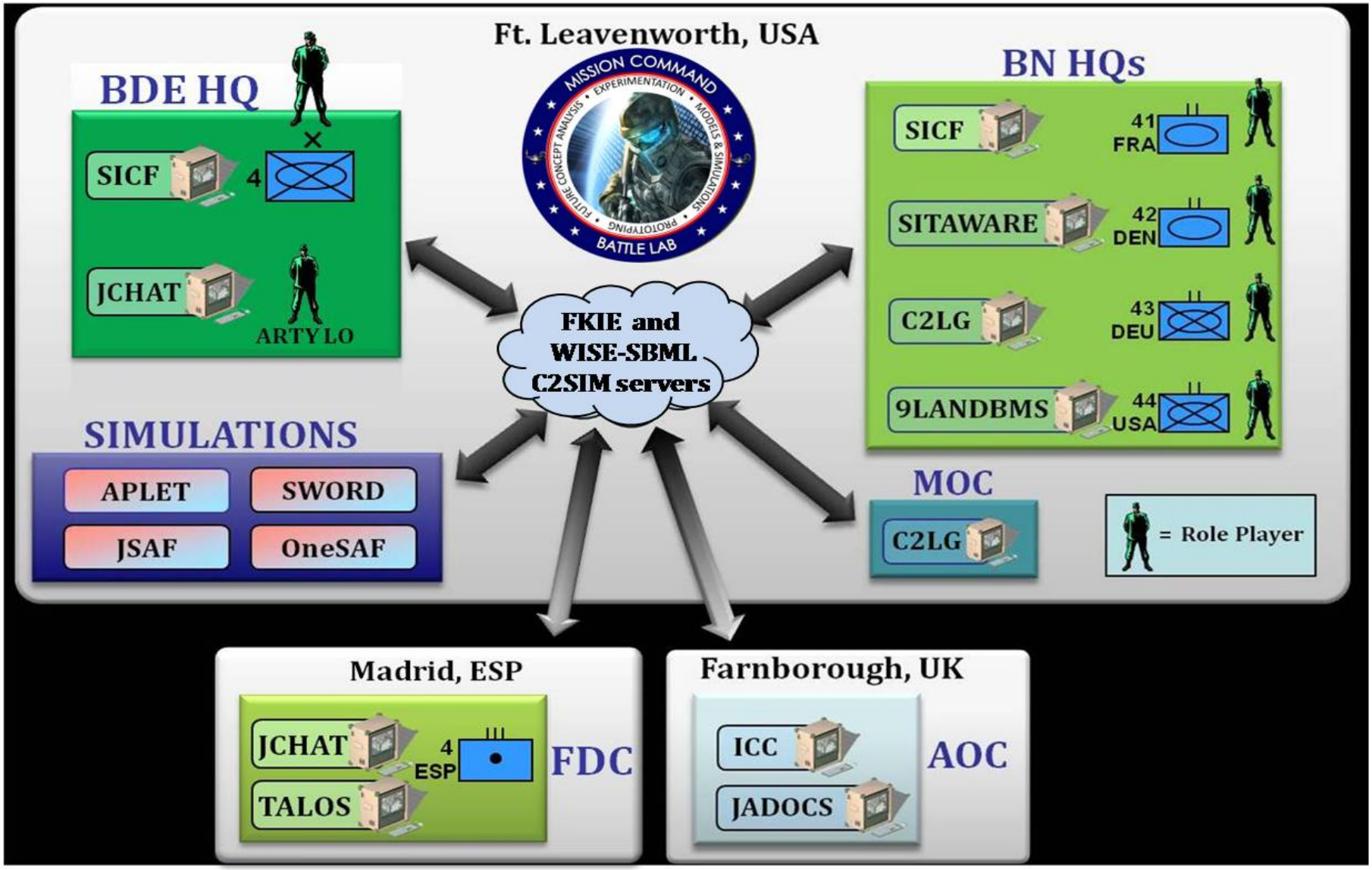
What Does C2SIM Enable

- "Train as you fight"
  - Using operational C2 systems
  - Eliminating human between C2 and simulation systems saves $$$
- Operational planning: COA analysis
- Operational mission rehearsal
- For Service, Joint and Coalition
- France using to support acquisition

C2SIM Basic Architecture



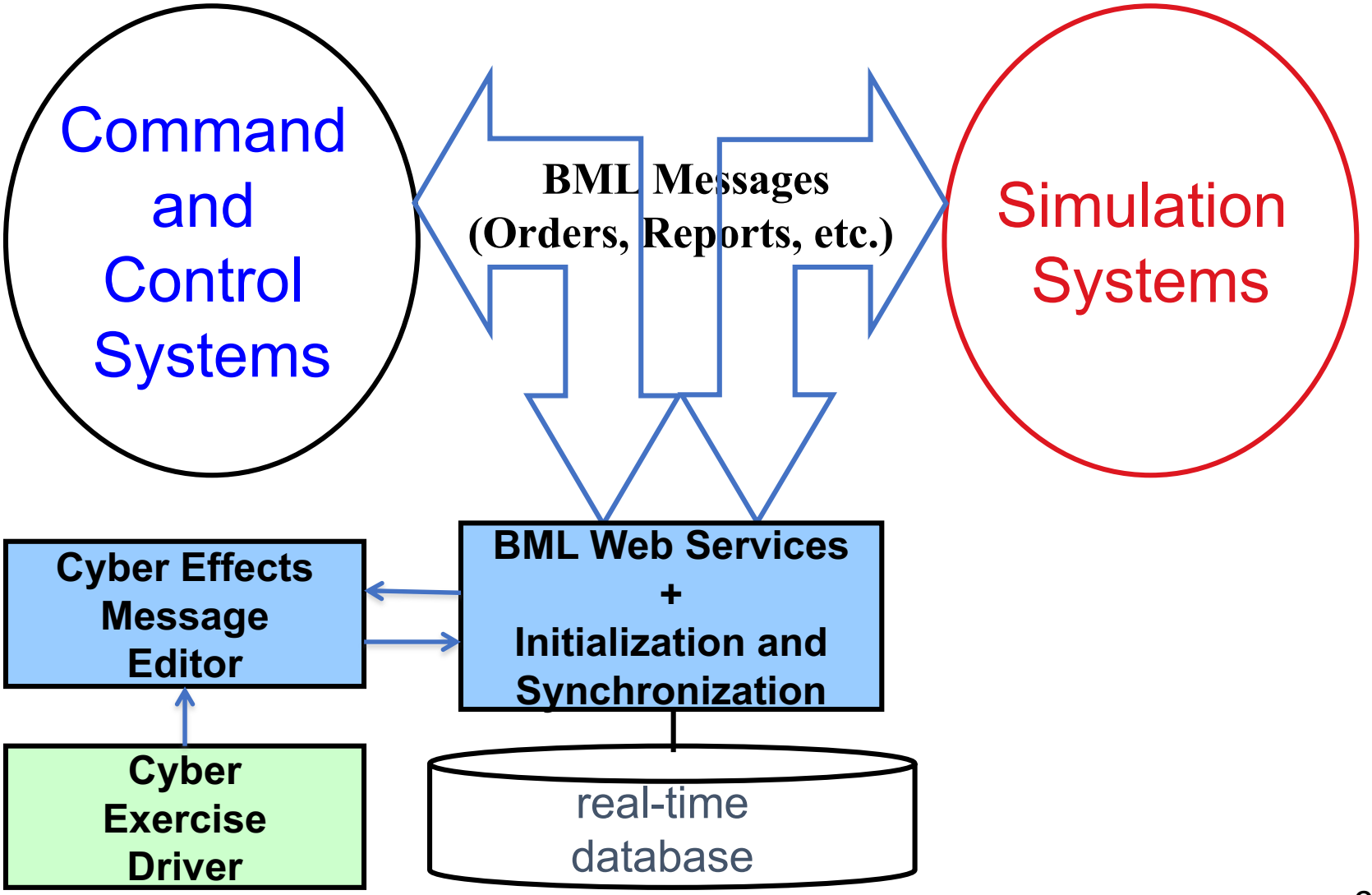
C2SIM Example:
MSG-085 Final Demonstration Architecture



Importance of Training in Cyber-Active Environments

- Two kinds of cybersecurity training:
  - Cyber specialists defending from (attacking?) adversaries
  - Operational military who may have to function under cyber-active conditions
- Second was tested in CWIX 2018 and is critical
  - Forces must not be crippled by cyber attack!
- Concern is for cyber + electronic warfare (CEMA) because impact on operations can be similar
- Actually compromising command and control (C2) would be very disruptive to training exercises
- Modifying the systems so they appear to be compromised is possible but expensive/time-consuming

C2SIM Cyber Effects in Operational Training
Expanded C2SIM Architecture



CWIX Testing Results

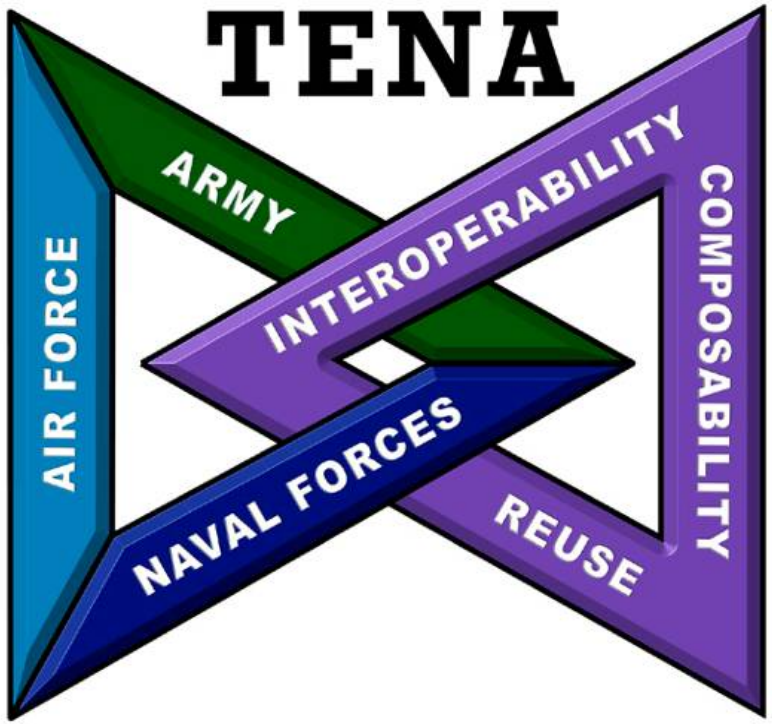
- Phase 0 Confirm network connections: (Major change from testing plan: three of the four CFBLNet sites were not available)
  - However we had fallback copies of VRForces and C2SIM Server
  - And a recorded trace of JSAF UAS reports (Blue and Red)
  - So we were able to carry out most planned testing
- Phase 1 Confirm server compatibility:
  - Success with all client-server connections except missing JSAF
- Phase 2 Test C2SIM interoperation among all systems:
  - Success with NORCCIS sending orders to KORA and VR-Forces and receiving orders
  - Use recorded reports from JSAF to provide background traffic
- Phase 3 All systems engaged simultaneously with cyber:
  - Successful with air, then ground; when testing ALL, found and fixed a bug
  - Cyber worked as expected

MSG-145 Experimentation, Mini-Exercise and CWIX 2019

- Validating ballotable SISO C2SIM standard
- More complete testing
- Multi-national brigade scenario
- SME role-players debriefed on cyber effects

QUESTIONS

TENA Retina Demonstration



TENA Software Development Agency

Why TENA in Cyber?

- 2015 NDAA specifies collaboration between DoD Components and DoD EAs for Cyber Training and Test Ranges to:
  - Ensure interoperability with other DoD training & test infrastructure (kinetic and non-kinetic)
  - Develop cyber test and training infrastructure interface standards and other technical and operational standards
  - Establish a standard language (data exchange protocol) for representing and communicating cyber event and threat data during a cyber-range event
- TRMC has a 18+ year history of using TENA to meet these requirements for non-cyber test and training
- TRMC is proposing leveraging TENA to meet above DepSecDef and NDAA requirements

Current TENA Cyber Efforts

Goal: Demonstrate TENA use and utility in a relevant Cyber Training Use Case

- Use Case development
- DECRE demonstration support
- TENA Retina proof of concept
- Cyber event OM development
- SISO Cyber M&S reference model Working Group support
- 2019 Cyber Range Biennial Integrated Plan inputs

What is TENA?

- An implemented open architecture that addresses common test and training range requirements
- An architecture that promotes interoperability reducing integration time and cost
  - Rapidly combine modular, composable sets of geographically distributed range resources to meet new testing and training missions
- An architecture that enables:
  - Standardization of data models and lexicons
  - Interoperability between inter- and intra-range assets
  - Integration of Live, Virtual, and Constructive assets (locally or distributed)
  - Integration of multiple vendors/providers
  - Elimination of proprietary interfaces to range instrumentation
  - Sharing and reuse of common capabilities across existing and new investments
  - Efficient incremental upgrades to test and training capabilities

TENA is DoD's kinetic range integration architecture

TENA at a Glance

- TENA is composed of several components:
  - Customizable **Object Models** that standardize information exchange
    - Domain-specific “data contracts” support interoperability between range resources throughout the event lifecycle
  - A Software Infrastructure, the **TENA Middleware,** for distributing objects
    - Interoperability-enabling software libraries, **auto-code generated** for 34+ operating system / compiler combinations and C++, Java, and .NET programming languages
    - **100% Government off the Shelf (GOTS)**
    - A suite of software and best practices **matured over 16+ years**
  - A common suite of **software tools and best practices** to support Event Planning, Execution, and Analysis functions
  - **Collaboration mechanisms** that facilitate sharing and reuse
  - **Subject Matter Experts** for distributed exercise and system integration

The purpose of TENA is to provide the necessary enterprise-wide architecture and the common software infrastructure to:

- Enable interoperability among range, C4ISR, and simulation systems used across ranges, HWIL facilities, and development laboratories
- Leverage range infrastructure investments across the DoD to keep pace with test and training range requirements
- Foster reuse of range assets and reduce cost of future developments

How TENA is currently Used In Test and Training Facilities

- Common specifications for test and training data
- Data Dissemination across variable applications, platforms, programming languages, networks, and classification levels
- Data Collection and Playback

Data Management

- Local and Remote Command and Control
- Health & Status Monitoring

Event Management

- Real-Time simulations
- Stimulation of live sensors and instrumentation
- Connecting non-interoperable inter- and intra-range systems

LVC Integration

- Eliminating proprietary interfaces to range instrumentation
- Sharing and reuse of common range tools and capabilities
- Online Collaboration and File Sharing

Sharing & Reuse

These activities are all relevant to cyber experiments

TENA Cyber Range Support
DECRE Support Requests / Tasks

- Enhance Event Management
  - Integrate TENA Console and Canary applications into DECRE environment
  - Identify and Integrate additional TRMC capabilities to help monitor/manage events and demonstrate TENA Value
- Enhance Event Monitoring and AAR Visualization
  - Investigate TENA interface for Visualization
  - Investigate TENA opportunities for ShotVAL (Blue Cell)
  - Investigate TENA interface for Red Cell Application
  - Develop and Integrate TENA Retina
- Automate Deployment/Configuration of environment
  - Work with TRMC personnel to provide information on capabilities to enhance DECRE
  - Work with DECRE and TRMC to determine potential standard configuration capability to help drive deployment and monitoring of configuration.

DECRE Training Environment Current State

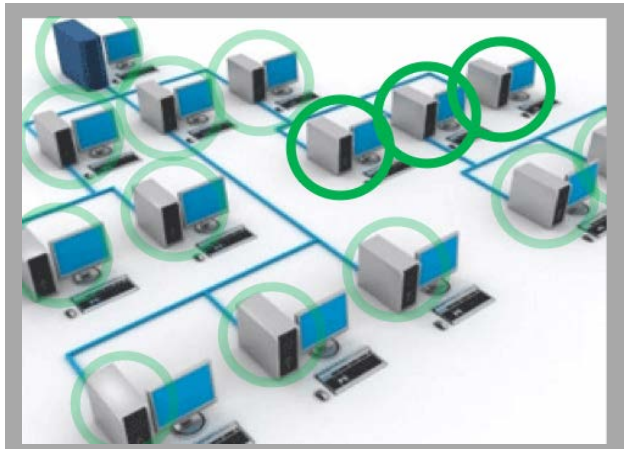
Gray Cell	Red Cell
	

Blue Cell	White Cell
	

ShotVal

DECRE Training Environment
TENA Enhanced

Gray Cell



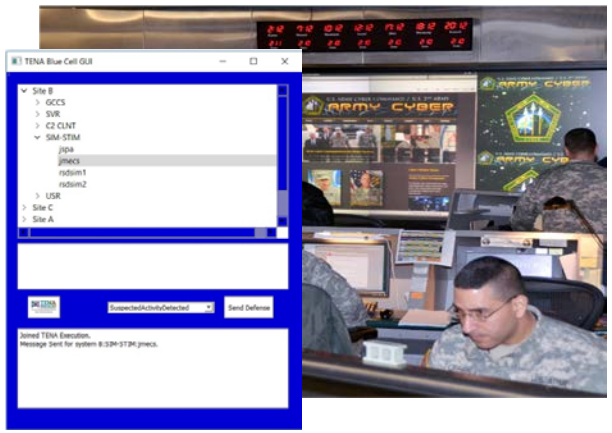
TENA System Sensors & Emulator

TENA System Monitor

solarwinds

Red Cell

Blue Cell

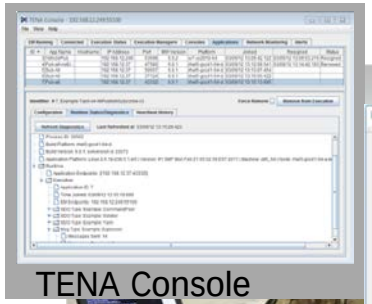


ShotVal

White Cell

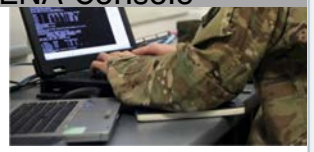
TENA

Chat Collector

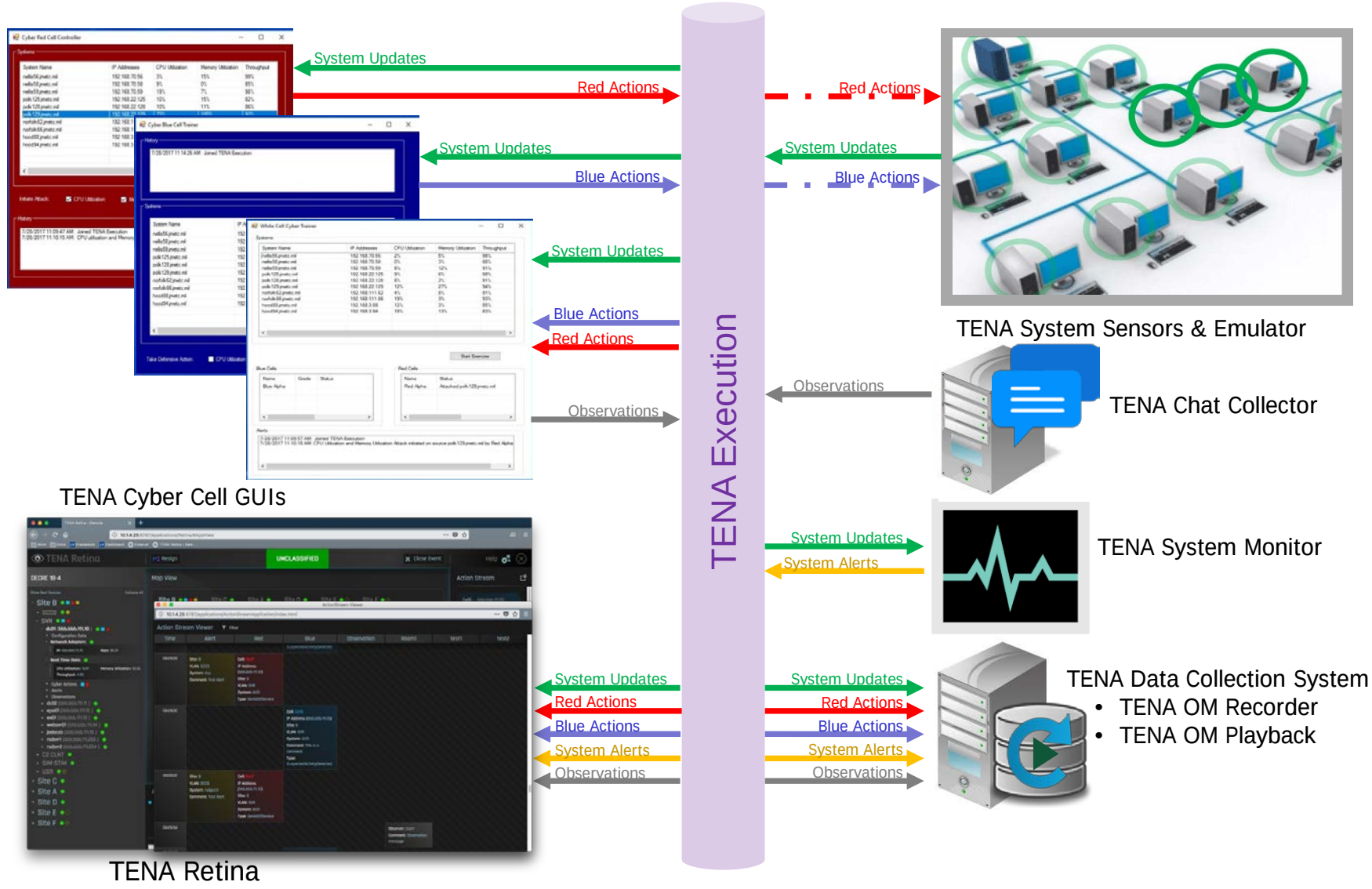


TENA Console

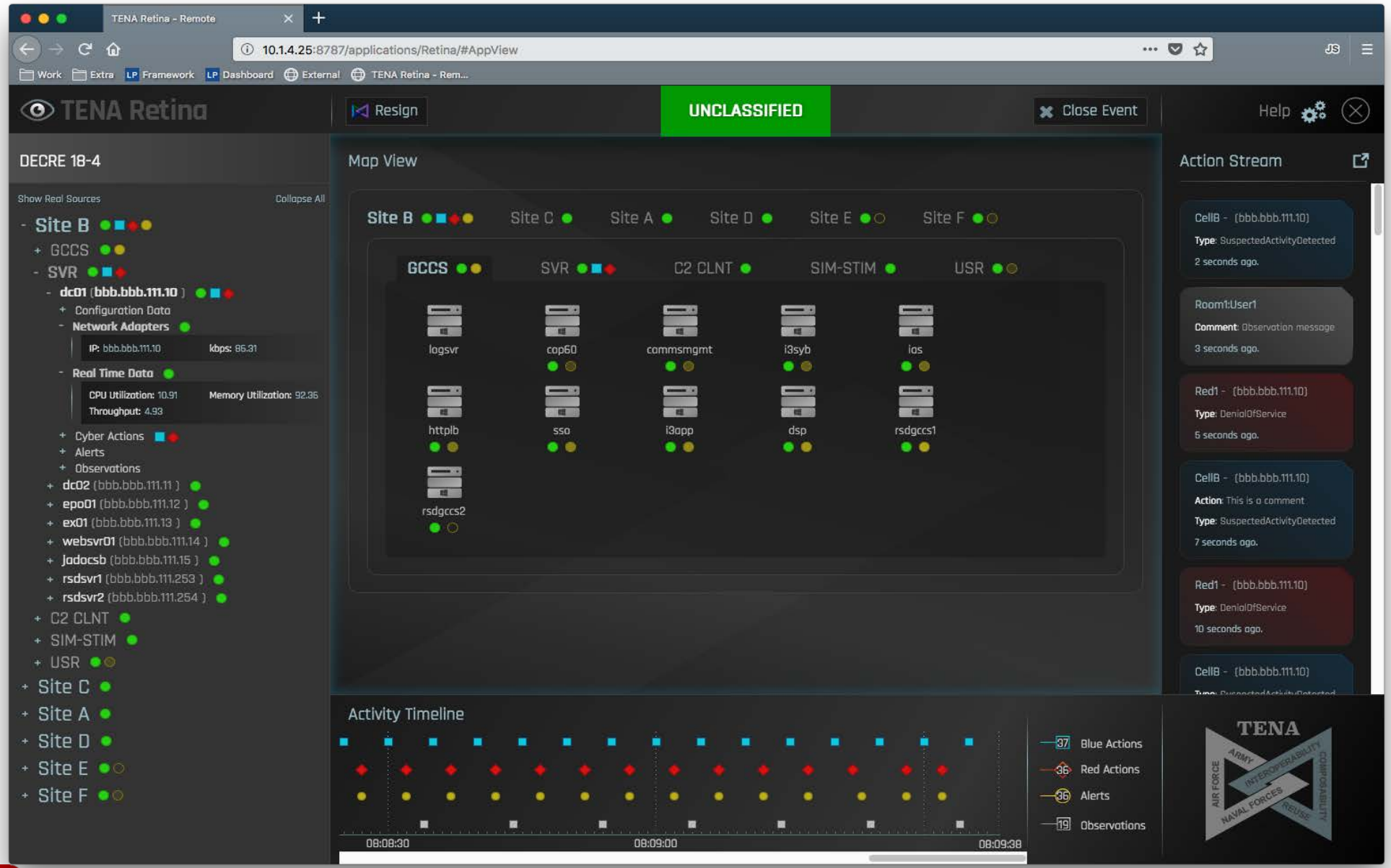
TDCS



TENA Cyber Range Support
Real-Time Data Flow



TENA Retina Demonstation



@IITSEC NTSAToday

TENA Cyber Range Support Conclusion

- TENA is a proven modular and open architecture that potentially meets the 2015 NDAA
- TENA is the DoD standard for integrated kinetic range systems for efficient T&E and training
- TENA provides a foundational architecture and capabilities for Cyber Test and Training
- TENA Retina event monitoring solution demonstrates the value of rapid development and integration in a cyber environment
- TENA provides a path to “advanced” event design / construction techniques
- Defining common data exchange models is critical to cyber test & training interoperability

TENA Cyber Range Support Conclusion

TENA Software Development Activity Director
Ryan Norman
(571) 372-2725
ryan.t.norman.civ@mail.mil

JMETC Program Manager
George Rumford
(571) 372-2724
george.j.rumford.civ@mail.mil

National Cyber Range Complex Director
AJ Pathmanathan
(571) 372-2702
arjuna.pathmanathan.civ@mail.mil

Event Scheduling / Event Questions

Interoperability Events
Keith Poch
(850) 389-6044
keith.poch@tena-sda.org

Distributed Tests
Linking Sites

Cyber Events
Lizann Messerschmidt
(571) 451-4295
lizann@mitre.org

NCR Events
RSDP Events

NCRC Expansion / Site Questions

NCRC, Deputy Director
Rob Tamburello
(501) 372-2753
robert.n.tamburello.civ@mail.mil

Connectivity / Network Questions

JMETC Secret Network (JSN)
Jeff Braget
(850) 389-6031
jeff.braget@tena-sda.org

Secret Only
Always Connected

JMETC MILS Network (JMN)
Ben Wilson
(757) 492-7621
bennett.wilson@navy.mil

Above Secret (TS/SCI/SAP)
Connected Only During Event

Range Support and Training

TENA User Support Manager
Gene Hudgins
(850) 803-3902
gene.hudgins@tena-sda.org

TENA Products / Software Repository

TENA Software Development Manager
Steve Bachinsky
(703) 253-1068
steve.bachinsky@tena-sda.org

JMETC Information Assurance Lead

Robin Deiulio
(540) 553-4098
Robin.deiulio.2.ctr@mail.mil

Miscellaneous Questions

For JMETC questions: feedback@jmetc.org
For TENA questions: feedback@tena-sda.org

Websites

Unclassified, FOUO, DoD-Restricted (CAC required): https://www.trmc.osd.mil
Distribution A, Industry, non-DoD (username/password required): https://www.tena-sda.org

Help Desk

Action Items, Questions, Tasks, Software Needs, Bug Reports: https://www.tena-sda.org/helpdesk

@IITSEC NTSAToday

JTEX-04: March 5-7, 2019; San Diego, CA

NTSA
I/ITSEC 2018
NOV 26TH – Nov 30TH | ORLANDO, FL
LAUNCHING INNOVATION IN LEARNING:
READY, SET, DISRUPT

Network Effects Emulation System (NE2S)

Jonathan Glass, NAWCTSD, NE2S Material Developer

Derek Bryan and Sean King, Ingenia Services, Inc., NE2S Contract Support

Requirement

"Execute more cyber (for others) training in Combatant Command exercises"

- "In the Marine Corps they say that every Marine is a rifleman. I say that everyone in the [Department of Defense] is a cyber warrior." (VADM Nancy Norton, Director DISA, Commander Joint Force HQ DODIN, CyberCon 2018)
- "Nearly all major acquisition programs that were operationally tested between 2012 and 2017 had mission-critical cyber vulnerabilities that adversaries could compromise." (GAO Report: Weapon System Cybersecurity Oct 2018)
- "#1 Objective: Ensuring the Joint Force can achieve its missions in a contested cyberspace environment." (US DOD Cyber Strategy 2018)
- "Given dramatic increases in the ability of adversaries to disrupt, degrade or destroy cyberspace and space systems, it is essential that the Joint Force be able to operate effectively despite degradation to those systems. Greater resilience must be built into technical architectures, and the force must regularly train to operate in "worst case" degraded environments." (CJCS Capstone Concept for Joint Operations: Joint Force 2020)

Roles & Responsibilities

- 2009-2014: Owned and developed by Joint Staff J7
- April 2014: Naval Air Warfare Center Training System Division (NAWCTSD) named material developer
- June 2017: Ingenia Services, Inc. awarded Phase 1 Computer Network Defense (CND) Trainer Small Business Innovative Research (SBIR) project (TPOC – NAWCTSD)
- December 2017: U.S. Indo-Pacific Command Cyber War Innovation Center named Program Manager (through 2019)
- October 2018: Ingenia Services, Inc. awarded Phase II CND Trainer SBIR

Overview

- NE2S is a software emulator that mimics host and network cyber-degraded effects on Windows-based end user workstations.
- The web-based Master Control Station (MCS) allows training and exercise personnel to command and control effects from any connected workstation (cloud compatible).
- The client application (requires DAA approval) must be installed on all target workstations.
- NE2S does not affect the underlying network or host infrastructure – mimics effects locally using client software.
- Effects can be instantly started/stopped from the MCS and will timeout if communications with MCS ceases.

A safe, secure, managed tool for introducing cyber-degraded effects. Provides leaders and staffs opportunities to develop, train, and exercise CONOPS/TTPs (e.g., PACE) for fighting through cyber-degraded environments.

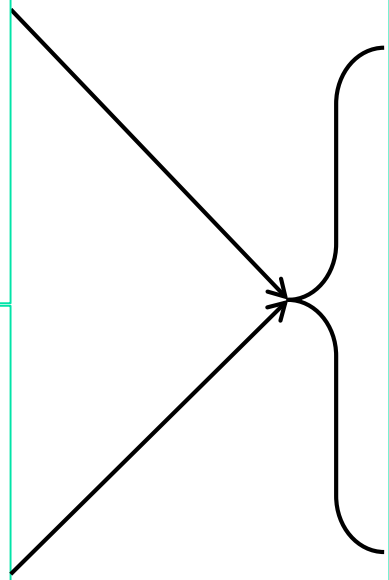
Effects

Host Effects

- Blue Screen
- Erratic Mouse
- Keyboard Lock
- Forced Reboot
- Sound Damage
- Disruption to Monitor
- CPU Usage
- Memory Usage
- Virus/Malware
- Ransomware

Network Effects

- Delay
- Jitter
- Packet Loss
- Packet Duplication
- Packet Corruption
- Packet Reordering
- Bandwidth Limitations
- Packet Filter
- Phishing

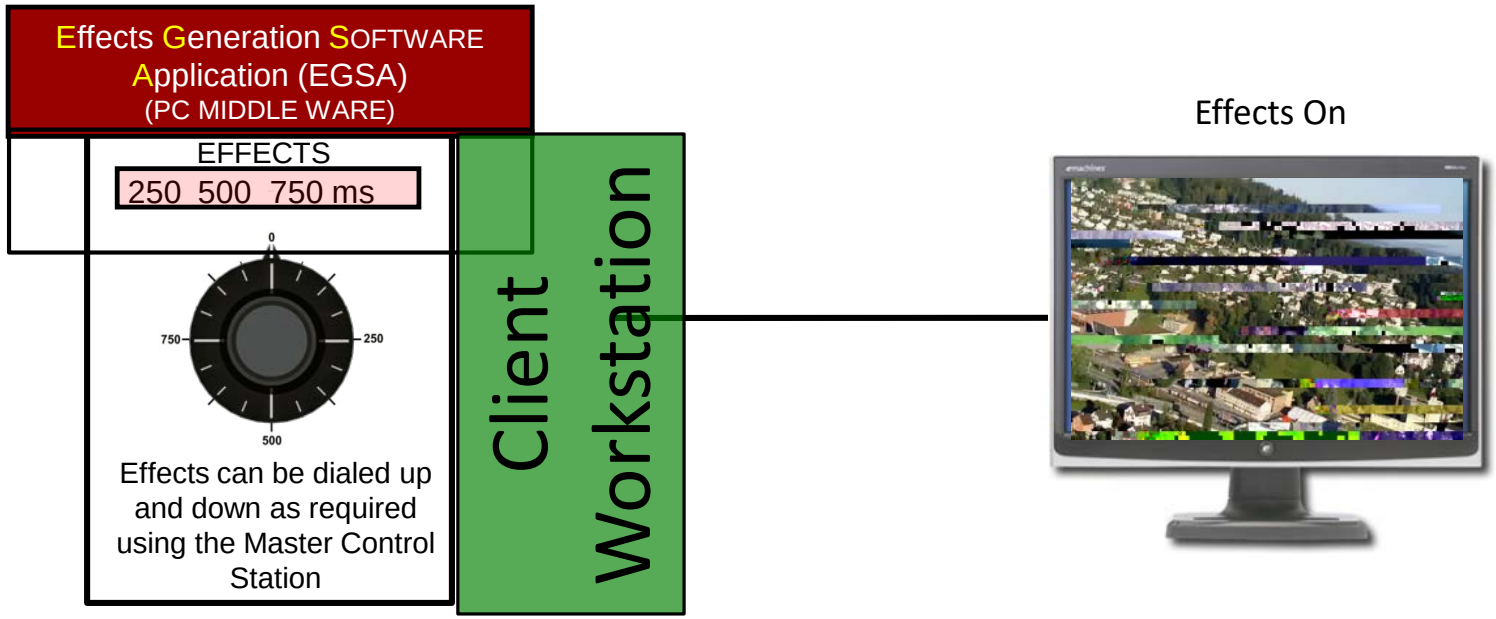


Operational Effects

- Annoyance/Frustration
- Work Delays/Stoppage
- Denial of Service (DoS)
  - Web
  - E-mail
  - Chat
  - Audio
  - Video
- Contingency Operations
- Computer Network Defense Operations

Effects (cont.)

- Effects are targeted by IP address, port, and protocol.
- Where applicable, effects can be “dialed up/down” to increase/decrease “pain.”
- Effects can be “chained” – Phishing e-mail that when successful (user clicks on fictitious link) triggers emulated network degradation.
- Effects can be planned and deployed hierarchically – individual workstation, groups of workstations, and/or groups of groups.



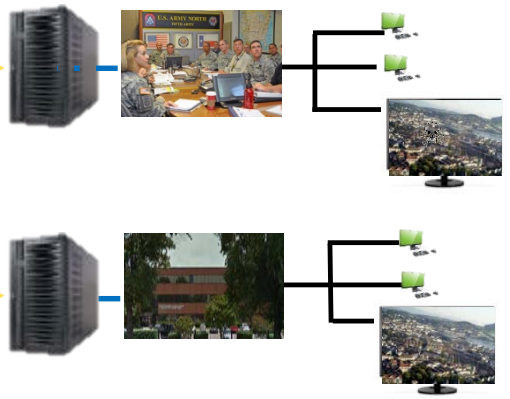
Architecture

NE2S Operator

TLS bi-directional authenticated encryption

MCS Server

TLS bi-directional authenticated encryption



Training Audience

Downloads / Users

- NE2S has been briefed and/or demonstrated to all Combatant Commands, the NATO Joint Force Training Centre, and the Canadian Forces Warfare Centre, among others.

- The following organizations currently have a copy of NE2S:
  - USNORTHCOM
  - USPACOM
  - I MEF
  - 15th Signal Brigade
  - Combined Arms Command
  - 505th Combat Training Squadron
  - ARCYBER
  - TRADOC
  - Electronic Proving Ground
  - ARNORTH
  - ARSTRAT
  - Naval Warfare Development Command
  - South Carolina National Guard

Versions

- 1.5 – Current official release
- 2.0 – Not fielded
  - Cloud-based architecture enhancements
- 2.2 – Available by request
  - Adds phishing effect
  - Adds Windows 10 client support
- 2.X – In production
  - Bug fixes
  - Improved installer
  - Red team findings
  - Virus / malware / ransomware
- Online, CAC-enabled collaborative development and distribution at - https://confluence.di2e.net/display/NE2S

Exercise Integration

- Cyber Operational Architecture Training System
  - 2014-2018: Demonstrate ability to receive and execute effects requests from a distributed cyber range environment
- U.S. Forces Korea
  - 2014-2015: Exercise Key Resolve
  - 2015: Exercise Ulchi Freedom Guardian
  - Demonstrate ability to degrade exercise Common Operational Picture (COP) and degrade exercise voice and video communications
- Operation Blended Warrior
  - 2016-2017: LVC technical demonstration at I/ITSEC
  - Demonstrate ability to degrade voice and video communications, workstations, and execute phishing campaigns against operations center systems
- Fleet Synthetic Training
  - 2017 LVC experiment
  - Demonstrate ability to degrade voice and video communications

Information Assurance

- JS J7 NIPR/SIPR ATO expired April 2017
- Red team testing conducted by the National Cyber Range
- Navy Risk Management Framework ATO process ongoing, expected NIPRNET and SIPRNET approval January 2019

10 Minute Break

Current Challenges and the Future of Cyber Training

- Get Started!
  - Existing requirements and guidance necessitate starting sooner rather than later
  - Learn through doing
  - Develop an incremental approach
  - The enemy will (eventually) decide for you if they haven't already
- "Knowing Is Half the Battle"
  - Seek guidance from the intelligence community on red cyber threats and effects
  - Seek guidance from the cyber operations community on blue cyber operations and effects
  - Seek guidance from the cyber training community on how to support and implement cyber training solutions

Current Challenges and the Future of Cyber Training

- "You Can't Fight in Here. This is the War Room!"
  - Information Assurance is often a schedule risk
  - Engage the IA community early and often
  - Encourage common sense approaches and reasonable mitigation strategies
  - Develop a backup plan
- Embedding Cyber Knife Fights into Exercises
  - Know your training objectives and training audience and carefully consider how best to address their requirements
  - Include external organizations when required, role play where appropriate
  - Don't over-design your solution

Current Challenges and the Future of Cyber Training

- Where Are the Standards?
  - Operations – CONPLANs/OPLANS, Joint Capability Areas, Joint and Service Mission Essential Task Lists
  - Readiness & Training – Objectives, Measures of Effectiveness/Performance
  - Test & Evaluation – Systems, Organizations, TTPs
  - M&S – Strategy, Policy, Interoperability

- What's On the Horizon?
  - National Cyber Range expansion
  - Persistent Cyber Training Environment
  - Improved cyber simulations/emulations
  - Cyber-aware LVC environments
  - Coalition cyber operations
  - Cyber/Electronic Warfare convergence
  - Multi-Domain Battle

Review

- Learning Objectives
  - Describe government requirements and guidance for conducting cyberspace training
  - Define and describe key cyberspace training audiences and outcomes
  - Define and describe key cyberspace training concepts and technologies
  - Explain the process of designing a cyberspace training environment
  - Describe the current challenges and future of cyberspace training
  - Demonstrate and experience critical cyberspace training tools

Summary/Conclusion

- Get started (the enemy has)
- Rely on your instincts and past experiences with traditional training programs and capabilities
- Crawl, walk, run
- Help is out there (but there aren't many of us)

Where Else Can I Find Help?

- OSD – Cyber Range Advisory Group, Cyber Range User's Guide, Cyber M&S Technical Working Group
- Joint Staff – DoD Enterprise Cyber Range Environment (DECRE)
- DOT&E – Cybersecurity Testing and Assessment, Cybersecurity Annual Report
- U.S. Indo-Pacific Command Cyber War Innovation Center (CWIC) – Cyber Testing, Training, and Experimentation
- U.S. Air Force 90th Cyberspace Operations Squadron – Cyber Capability Development, Testing and Training
- U.S. Army – EA for Cyber Training Ranges, Persistent Cyber Training Environment, Cyber/EW M&S Working Group
- Test Resource Management Center – Executive Agent (EA) for Cyber Test Ranges, Cyber Range Interoperability Standards (CRIS) Working Group, National Cyber Range Complex
- Simulation Interoperability Standards Organization's (SISO) Cyber M&S Study Group
- NATO Cooperative Cyber Defence Centre of Excellence

Cyberspace Training – Yes It's Legal!

Will Someone Please Tell the IA Officer?

Dr. David "Fuzzy" Wells, Deputy Director, UCF Institute for Simulation and Training
Derek Bryan, USINDOPACOM J81/Ingenia Services, Inc.

INSTITUTE for SIMULATION & TRAINING

UNITED STATES INDO-PACIFIC COMMAND
CYBER WAR INNOVATION CENTER

Q&A