U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – SOLDIER CENTER

Cyber Augmented Operations Technical Symposium 2019: CyberBOSS Overview

Dr. Omar Hasan
Dignitas Technologies, LLC
3504 Lake Lynda Drive
Building 20, Suite 170
Orlando, FL 32817
V: 407-601-7847
info@dignitastechnologies.com

Kevin Hofstra
CyberCENTS
Metova Federal, LLC
cybercents.sales@metova.com

Govt. Lead:
Nathan Vey
(407)208-3392
nathan.l.vey.civ@mail.mil

Simulation and Training Technology Center (STTC)

CYBERBOSS OBJECTIVES

Broker Cyber Actions and Effects Across LVC&G Systems

- Adjudicate cyber effects between federates to enable fair-fight concepts

Use a Services Approach to Develop a Cyber Terrain Ecosystem

- Open and Transparent – easy to see what is happening internally
- Flexible and Extensible – adaptable to future needs and/or third party extension

Define Common Data Model for Cyber Events

- Leverage existing models (e.g. COATS)
- Incorporate cyber-specific information (e.g. intentions, cyber-attacks, and cyber control)

Correlate Cyber Terrain between Synthetic Battlespaces

- Common device representation across federated LVC&G simulations and/or cyber ranges (e.g. CyberCENTS)

CENTRAL CONTROL AND ROUTING OF CYBER EFFECTS

CyberMaster | Cyber Role Player | Cyber Common Operating Picture (COP) | Cyber AAR | Cyber Exercise Creation Tools

Cyber Simulation Operator

Cyber Training GUIs

Metova Federal is a CyberBOSS team member

Metova CyberCENTS

Cyber Range Operator

Range Training Tools ↔ Other Cyber Ranges

CyberBOSS

- Common cyber effects definition
- Cyber event control strategy
- Cyber actor lists
- Cyber objects and infrastructure definitions
- Information message routing

CyberBOSS Interface Framework (CIF)

COBWebS — OneSAF (CyberBOSS Interface Framework)

COBWebS — JLCCTC (CyberBOSS Interface Framework)

Others (CyberBOSS Interface Framework)

Existing Simulation Systems

Live Simulation Systems

Synthetic Simulation Systems — COBWebS

Tactical Internet

Operational Devices

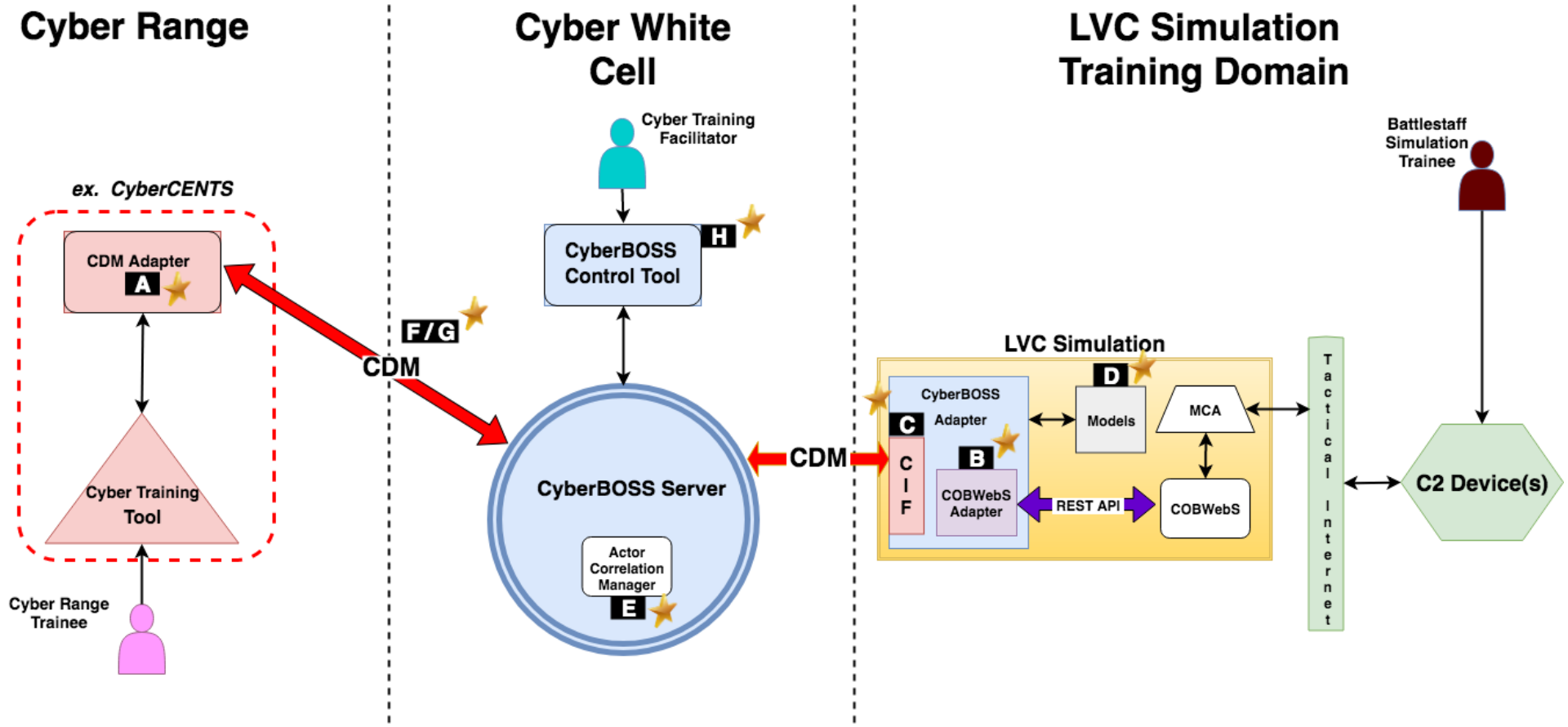
Cyber Effects Models

ICATS

TA / Battle Command Staff

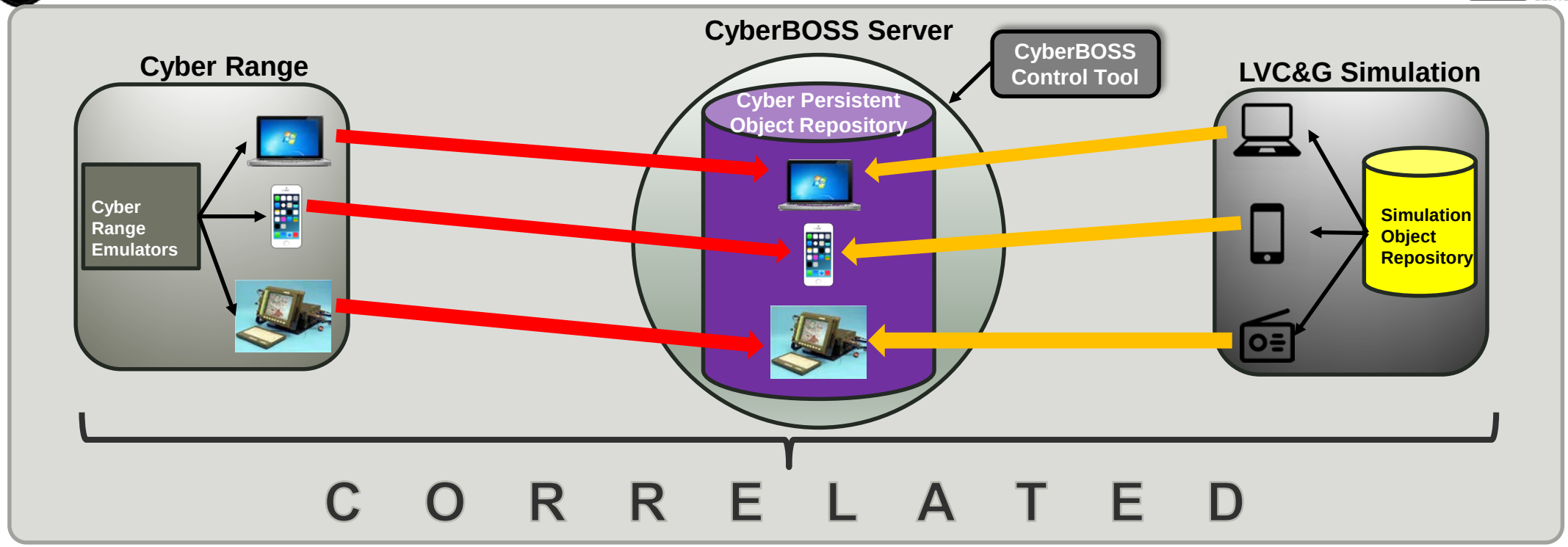
The CIF provides a client oriented perspective of the services and data in the CyberBOSS ecosystem

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

DEVICE CORRELATION



Disjoint Representation of Devices between CyberBOSS Federates

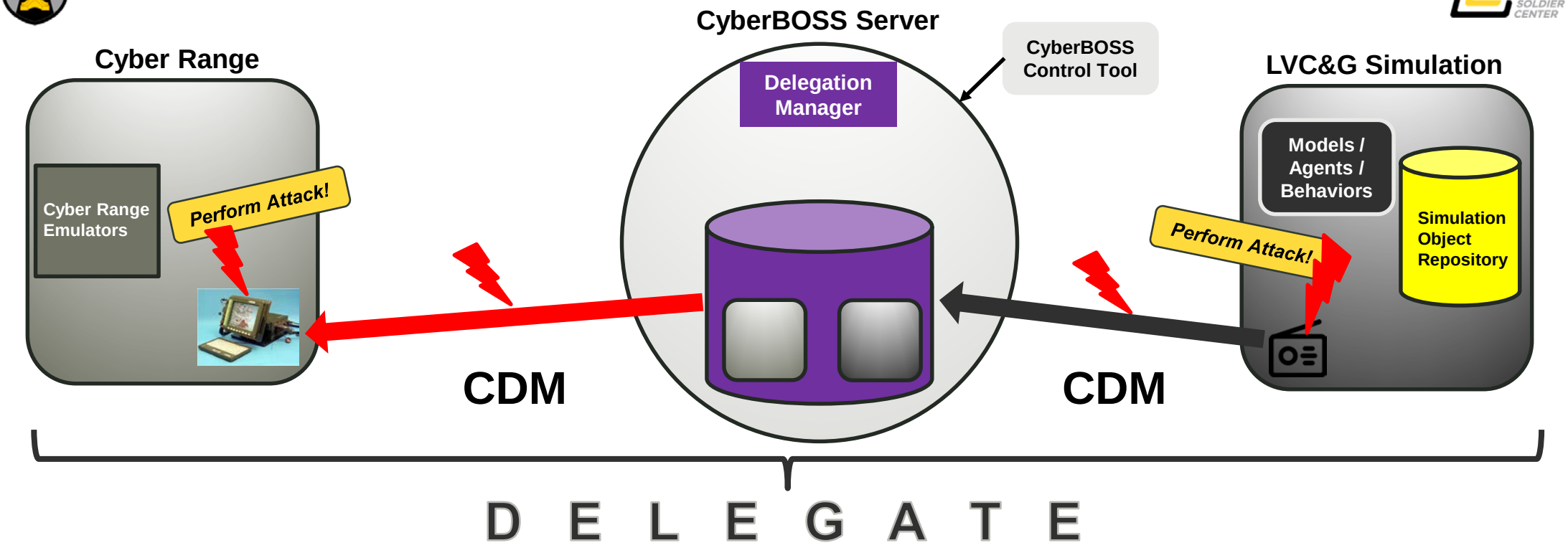
- Simulations use different information to refer to the same device
  - Cyber range represents operating system & version information
  - LVC&G simulation provides location information (tied to owning entity)

CyberBOSS Server Correlates Device Information between Federates

- Adjudicates information from all federates
  - Supports bridging device effects between the connected applications

Correlate Devices between Federates

CYBER EVENT DELEGATION



Harness Correlated Object Representation to Delegate Requests

- E.g. Issue task in LVC&G simulation, but delegate to federate with a higher fidelity representation

Adjudication / Routing Capability in CyberBOSS Server

- Actions are directed to the domain where they are best suited
- E.g. Cyber attacks should route to a cyber range if it is part of the federate

Route Cyber Events between Federates

QUESTIONS?

Govt. Lead:
Nathan Vey
(407)208-3392
nathan.l.vey.civ@mail.mil

CCDC – Soldier Center
Simulation & Training Technology Center (STTC)

Presenters

Dr. Omar Hasan
Dignitas Technologies, LLC
3504 Lake Lynda Drive
Building 20, Suite 170
Orlando, FL 32817
V: 407-601-7847
info@dignitastechnologies.com

Kevin Hofstra
CyberCENTS
Metova Federal, LLC
cybercents.sales@metova.com

BACKUP SLIDES

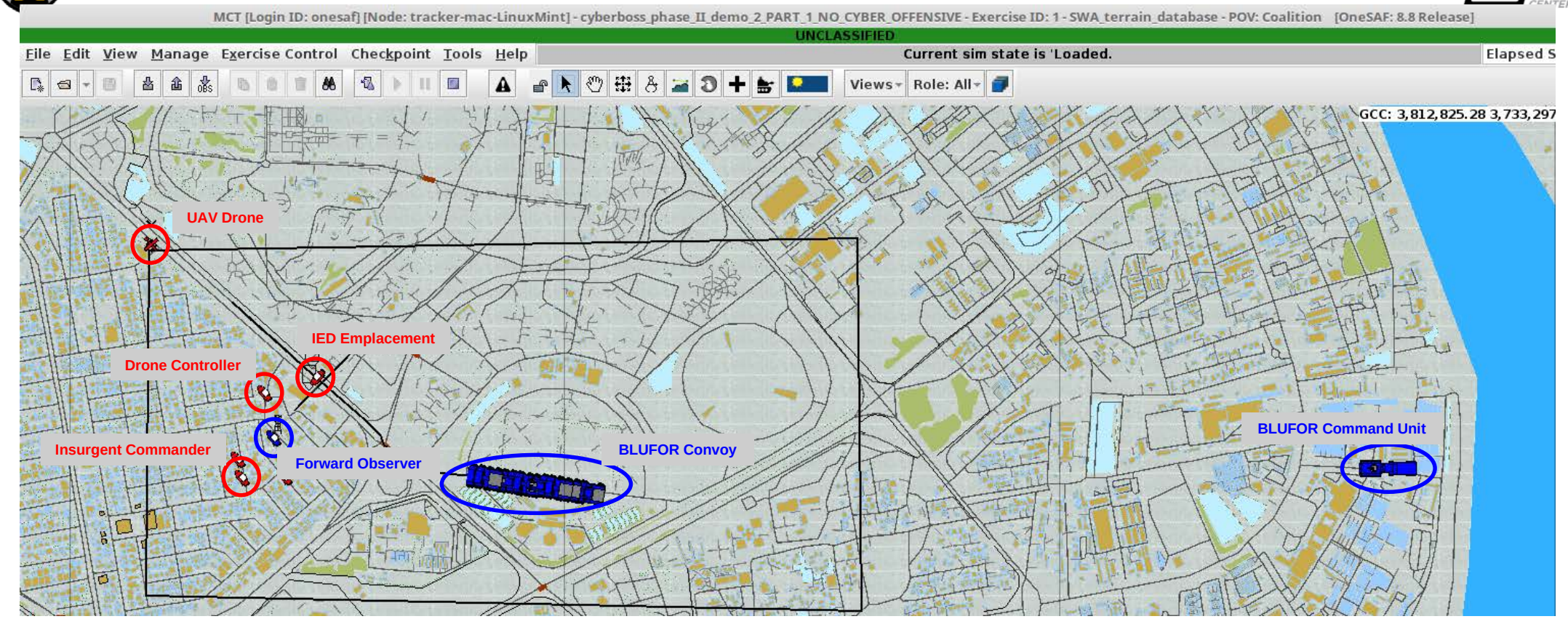
DEMO OBJECTIVES

- Incorporate cross-domain communication with CyberBOSS as a broker
  - Reconnaissance & Attack operations interoperate over disjoint applications (LVC & Cyber Range)
  - Demonstrate connections to the Cyber Range.
- Develop more complex scenarios that support offensive cyber training
- Extend Cyber Data Model (CDM) expression to support more robust client integration.
- Prototype the CyberBOSS Interface Framework (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

Scenario Description *Part 1*:

NO Offensive Cyber Attack

DEMO PART 1: *NO* CYBER OFFENSIVE

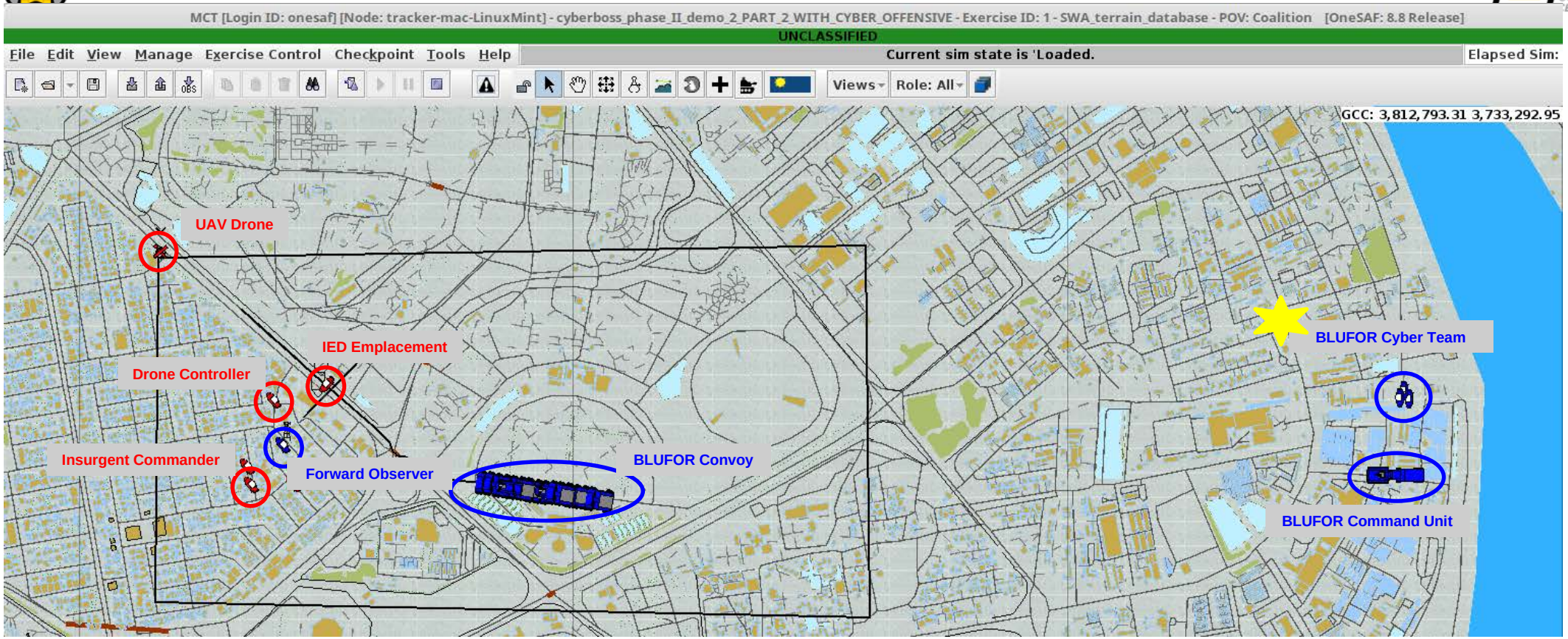


- **Part 1: *No* BLUFOR Cyber Offensive**
  - BLUFOR convoy traveling down route in urban environment
  - OPFOR insurgents situated in WiFi cafes, using a drone to surveil convoy activity
  - Commander instructs movement of Convoy, unaware of Insurgency coordinated IED attack
    - DoS on BLUFOR Commander's 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

Scenario Description *Part 2*:

WITH Offensive Cyber Attack

DEMO PART 2: *WITH* CYBER OFFENSIVE



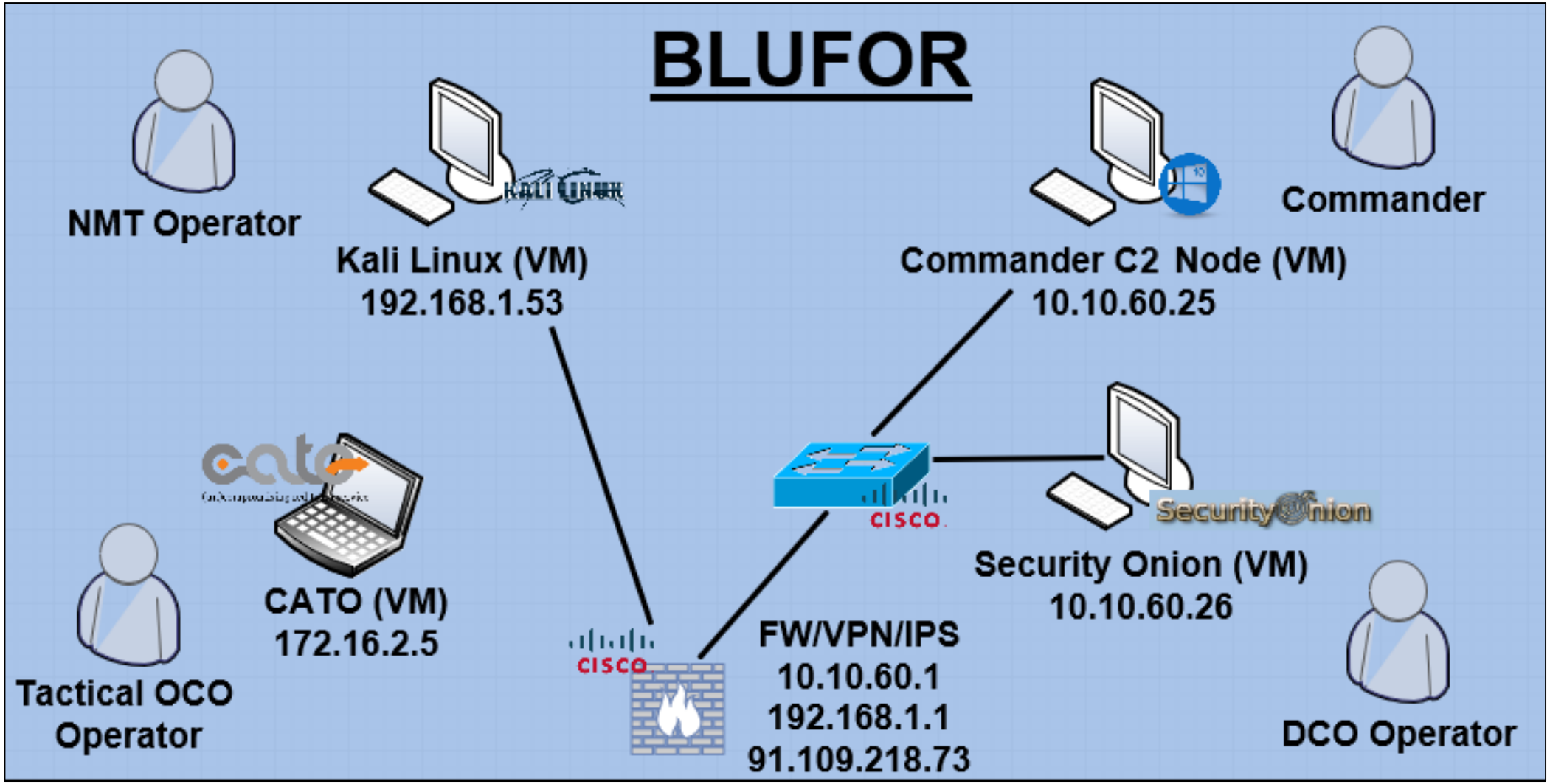
Part 2: *With* BLUFOR Cyber Offensive

- 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 drone and can no longer surveil the BLUFOR convoy
- OPFOR cannot initiate IED
- BLUFOR convoy moves through area unharmed.

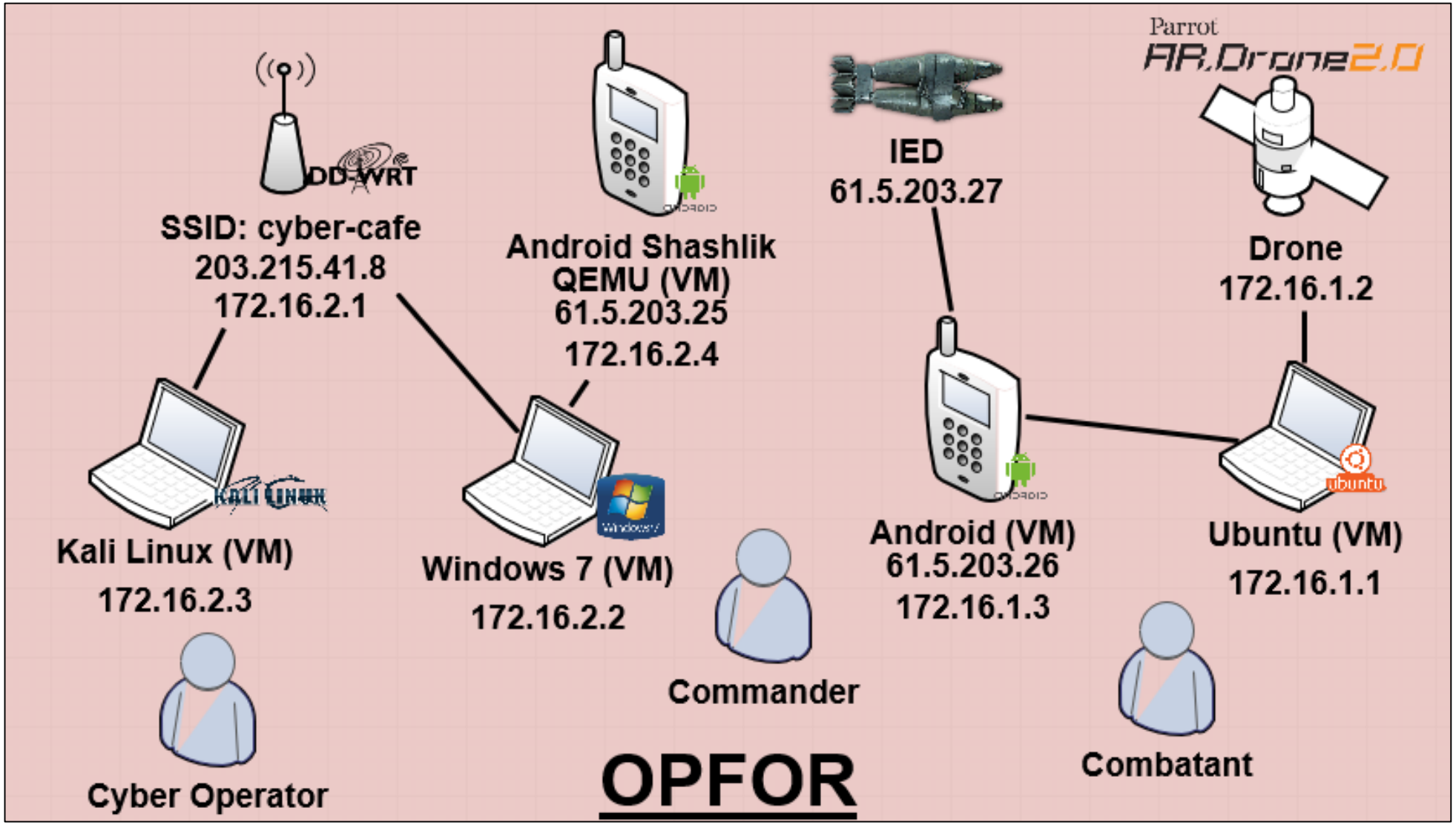
KEY OBJECTIVES

- 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 PART 2: BLUFOR CYBER ENTITIES



DEMO PART 2: OPFOR CYBER ENTITIES



DEMO PART 2: CYBER BATTLESPACE