Cyber Virtual Training

NDIA CYBER AUGMENTED OPERATIONS SYMPOSIUM

26 March 2019

Ambrose Kam

ambrose.kam@lmco.com

Cyber Innovations

Ambrose Kam

- **Over 24 yrs in Modeling & Simulation (M&S) and Operations Analysis (OA) with broad expertise in communications, networking, mission planning, renewable energy, radar, cyber, etc.**
- **Pioneer in applying M&S and OA techniques to cyber threat analysis.**
- **MIT Fellow in Systems Design & Management since 2002**
- **LM Fellow in Cyber**
- **2017 Asian American Engineer of the Year (AAEOY)**
- **Published over 30 research papers on a variety of subjects; guest lecturer @ MIT and Georgia Tech; industry internship sponsor/project lead on research projects with military academies**
- **MEng from Cornell; Dual Master's Degree from MIT (Systems Engineering & Management) Bachelor of Science from University at Buffalo**

Cyber Virtual Training in a Multi-Domain Op (MDO) Environment)

Real-Time Simulation-Based Operator-in-the-Loop

https://www.lockheedmartin.com/en-us/news/features/2016/webt-navy-area-51.html

Lockheed Martin Image

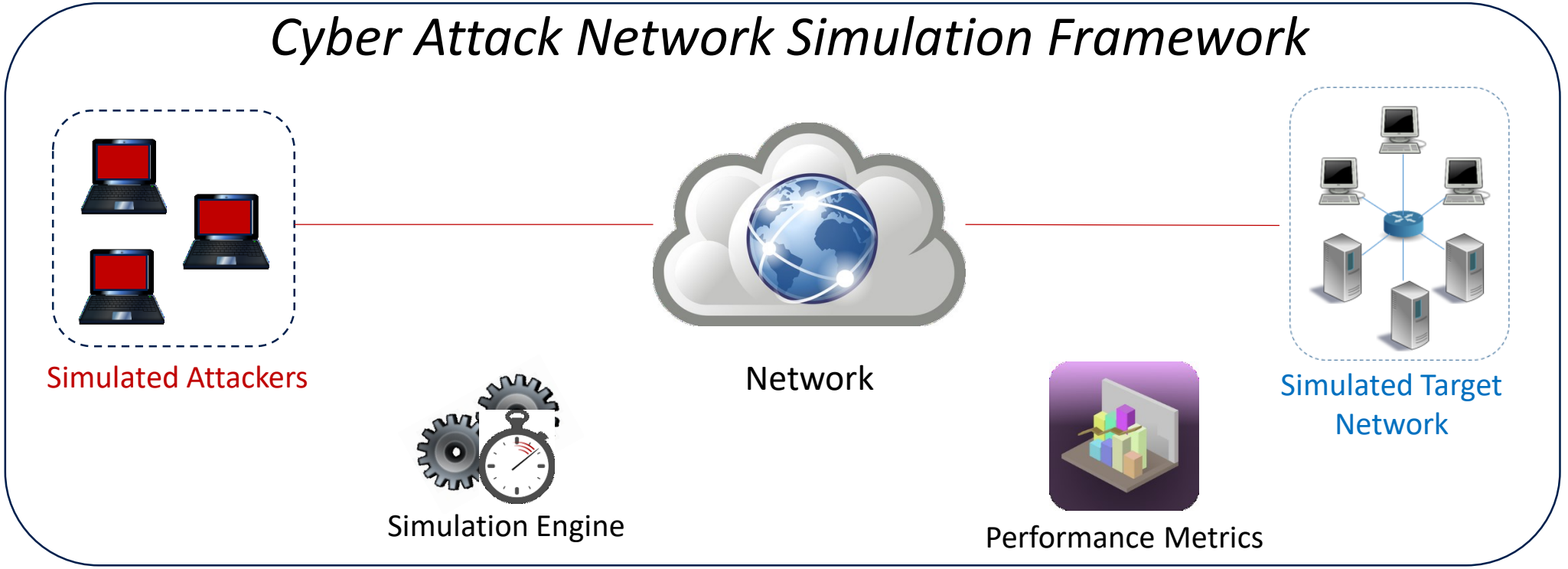
Motivations

- Objectives
  - Develop an operator-in-the-loop capability to support a wargaming environment; the goal is to determine how EW/Cyber TTPs affects mission effectiveness for both Red/Blue teams

- Problem Statement
  - Multi-domain Operations (MDO) is a big challenge; EW/Cyber will only make MDO more complicated given the quick advancement of the EW/Cyber techniques. Recent conflicts in Georgia and Ukraine showed how EW/Cyber can compliment traditional weaponry. US cannot afford to be left behind.

**Disclaimers: The example shown in this presentation is unclassified; it is not intended to represent any domestic or foreign systems/platforms.*

What is Cyber Attack Network Simulation (CANS)?

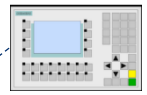


Lockheed Martin Image

The Cyber Attack Network Simulator (CANS) is a discrete event simulation that allows analysts to study the effect of various cyber events against a model of a planned or operational network system.

CANS models cyber events and their impacts to a system

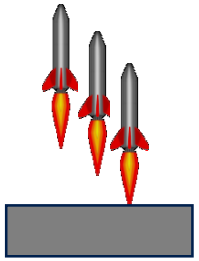
CANS Example



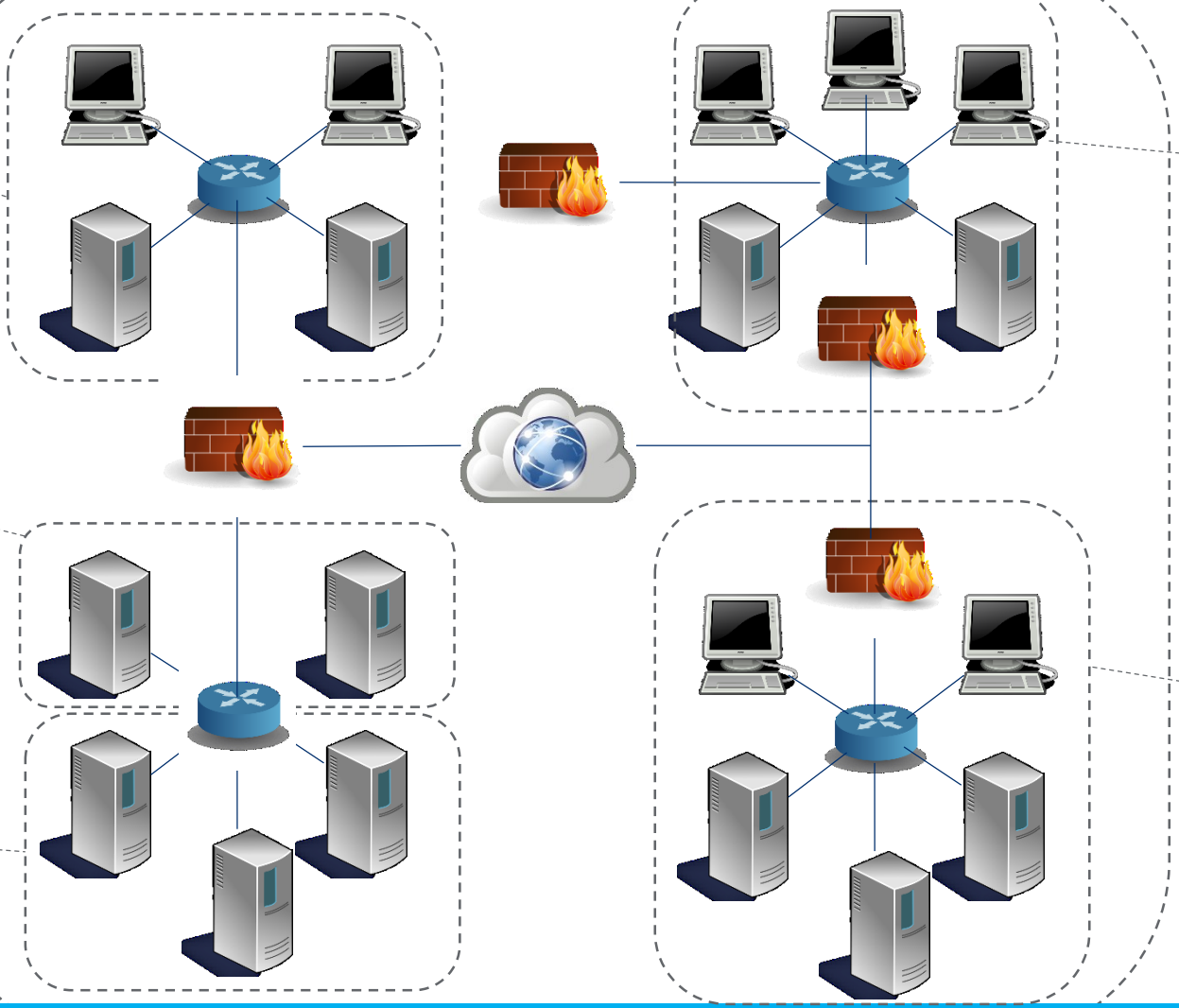
Operator Consoles

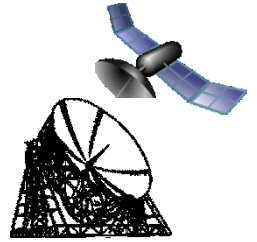
Destroyer

Sensor Systems



Weapon Systems





Satellite / Ground Station

Fighter Plane

CANS System Models are Highly Modular

What is AFSIM?

- Advanced Framework for Simulation, Integration & Modeling
- Government Owned object-oriented C++ library
- Discrete Event Simulation
- Can run at, faster and slower than real time
  - Can be Human-in-the-loop

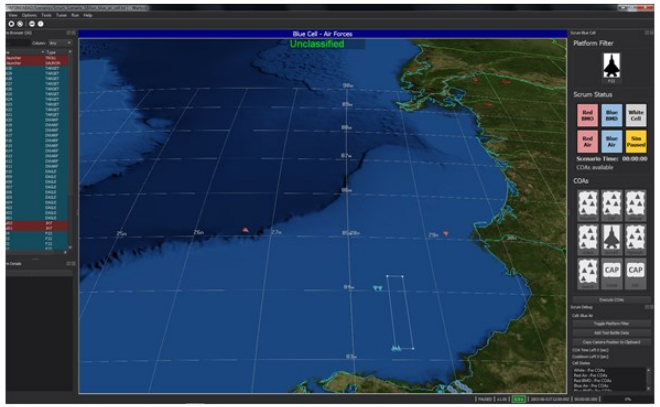
The intent of AFSIM is not to provide all encompassing models, but rather to provide the framework for incorporating the necessary models*

***from AFRL**

AFSIM Warlock Operator Interface

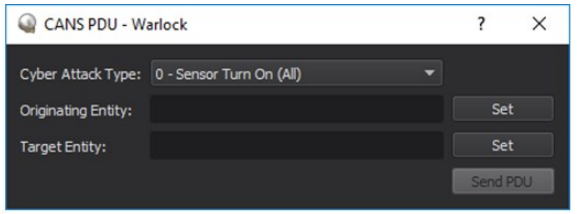
Courtesy of IST

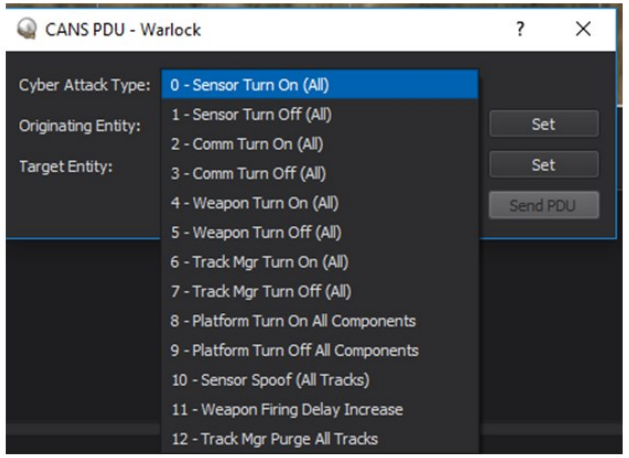
Distributed Operator Stations



Blue Cell Player

Courtesy of IST

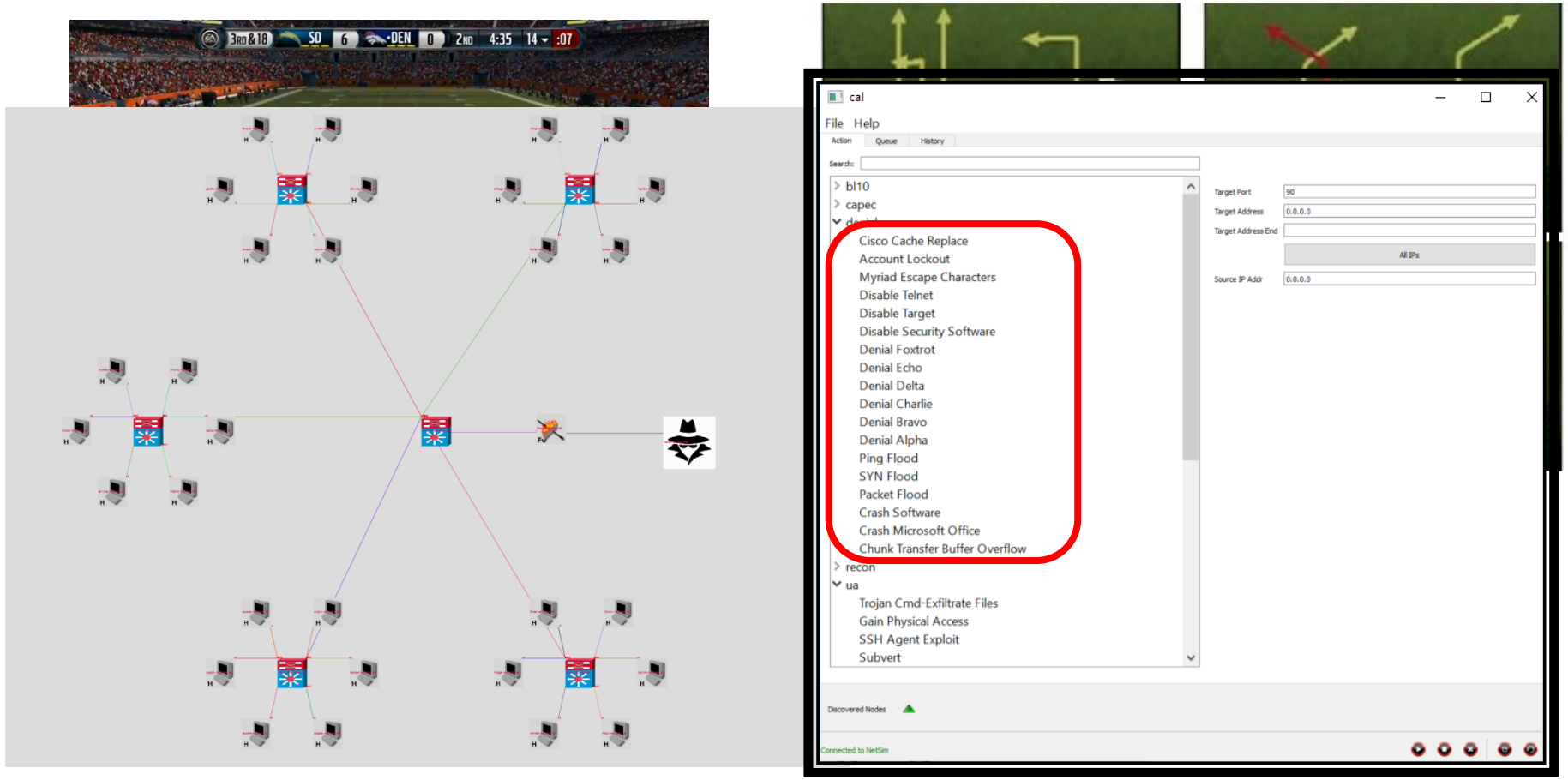


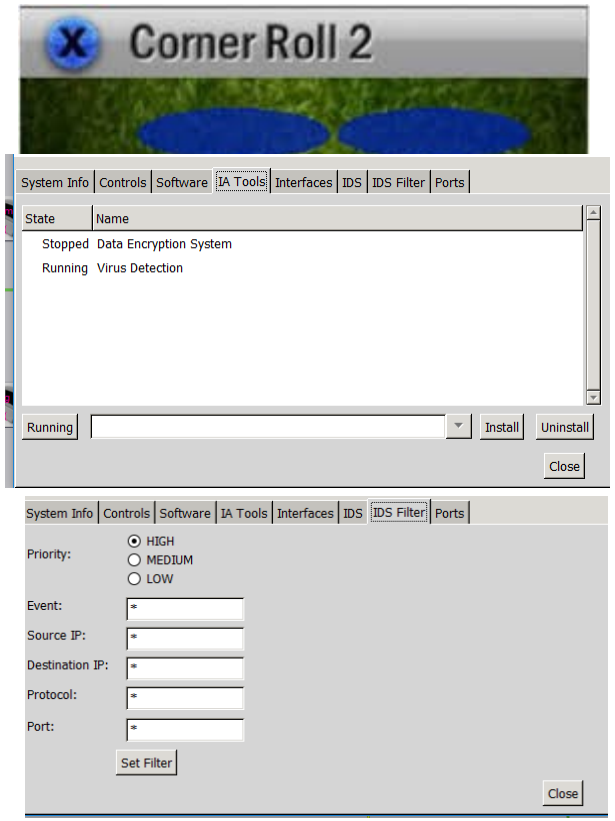


CANS/AFSIM DIS

Lockheed Martin Image

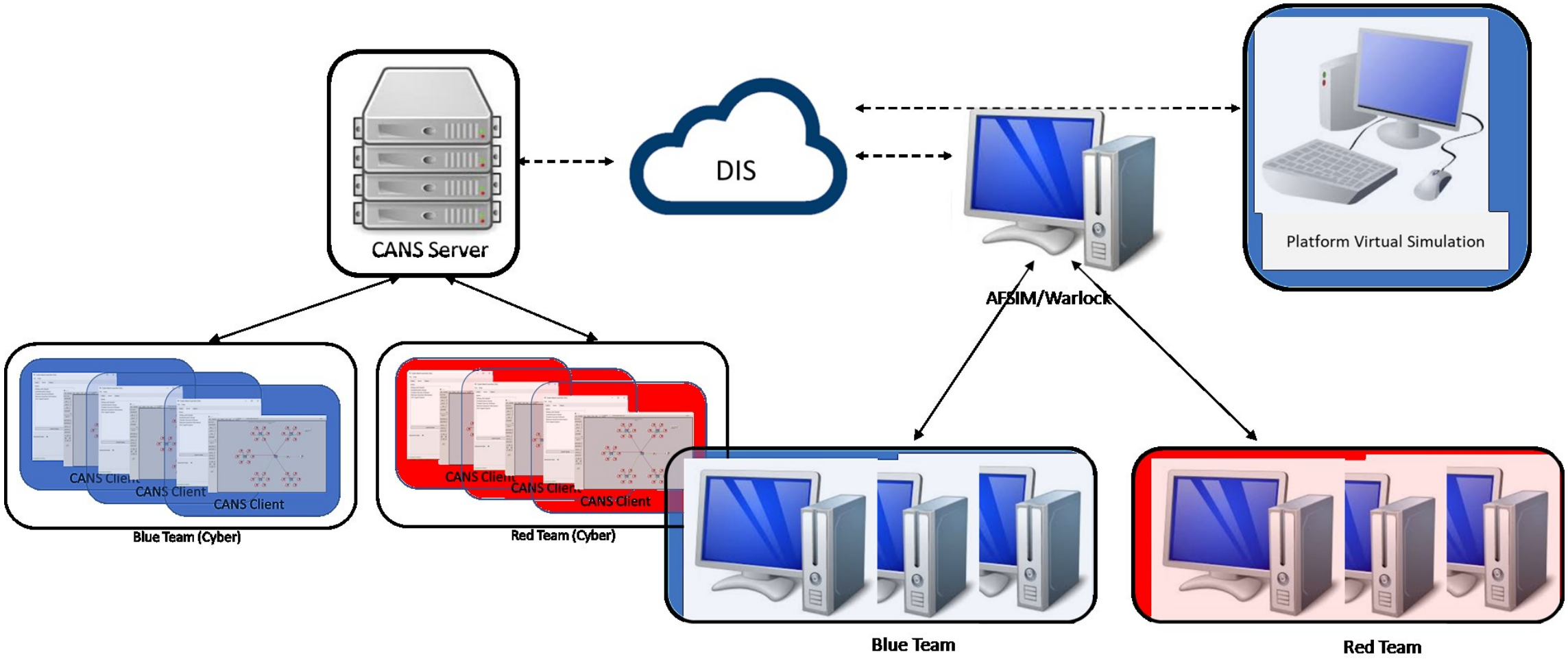
EW/Cyber Wargaming: A Madden Football Analogy





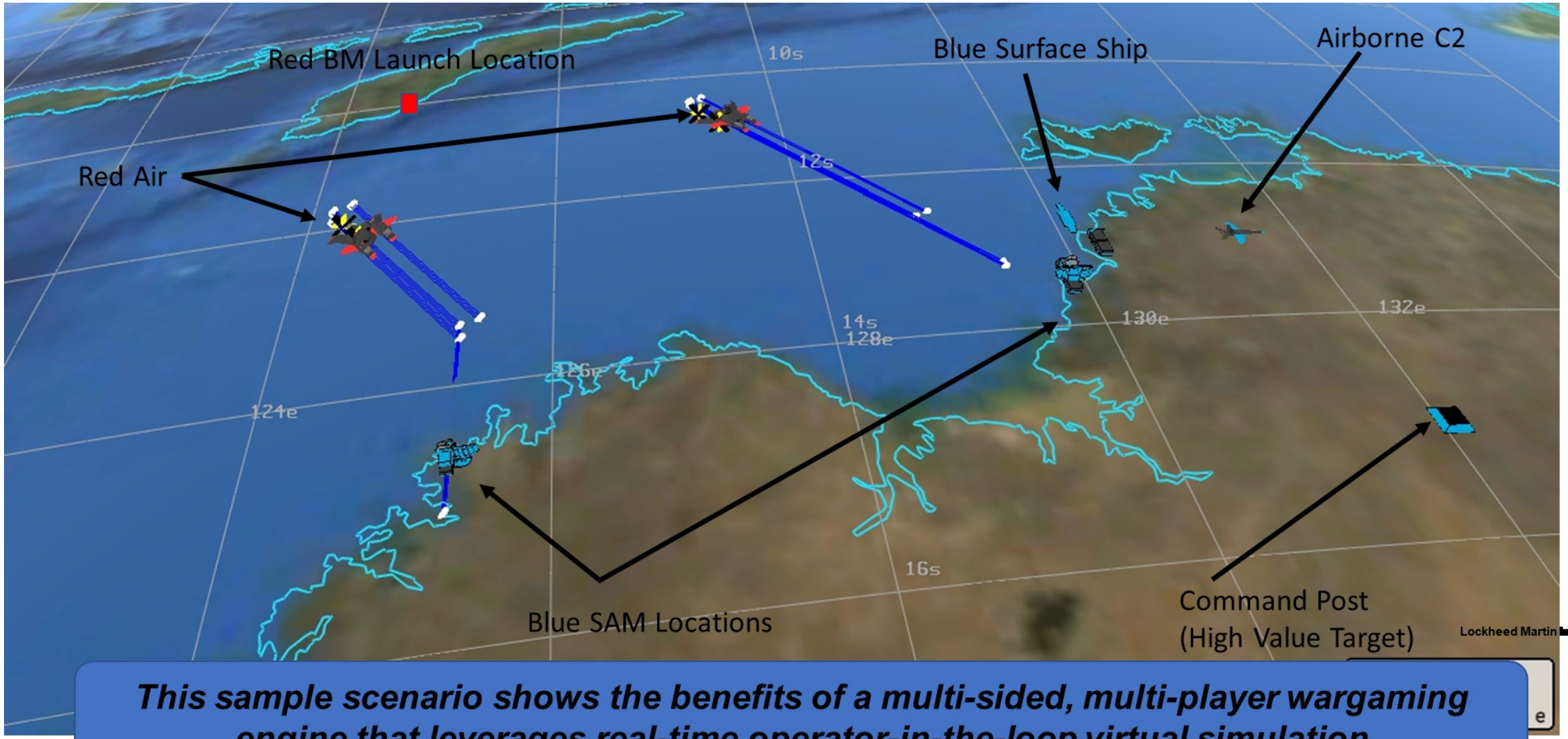
Lockheed Martin Image

CANS/AFSIM Software Architecture



Lockheed Martin Image

MDO Scenario OV-1



This sample scenario shows the benefits of a multi-sided, multi-player wargaming engine that leverages real-time operator-in-the-loop virtual simulation

Conclusion

- CANS/AFSIM Multi-Domain Wargaming Framework
  - Low Cost, Real-Time, Operator-in-the-Loop Wargaming Engine
  - Flexible scenario implementations to expose operational & capability gaps
  - Experiment with new Tactics, Techniques and Procedures (TTP)
  - Large variety of EW/Cyber exploits (offensive/defensive)

- Future Work
  - UCI messaging to bring in tactical systems
  - Mission planning tool integration
  - Artificial Intelligence, machine learning and optimization via AFSIM plug-ins

Questions?