# **Cyber Virtual Training**

#### NDIA CYBER AUGMENTED OPERATIONS SYMPOSIUM

26 March 2019

Ambrose Kam

ambrose.kam@lmco.com

**Cyber Innovations** 



Copyright © 2019 Lockheed Martin Corporation





#### 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

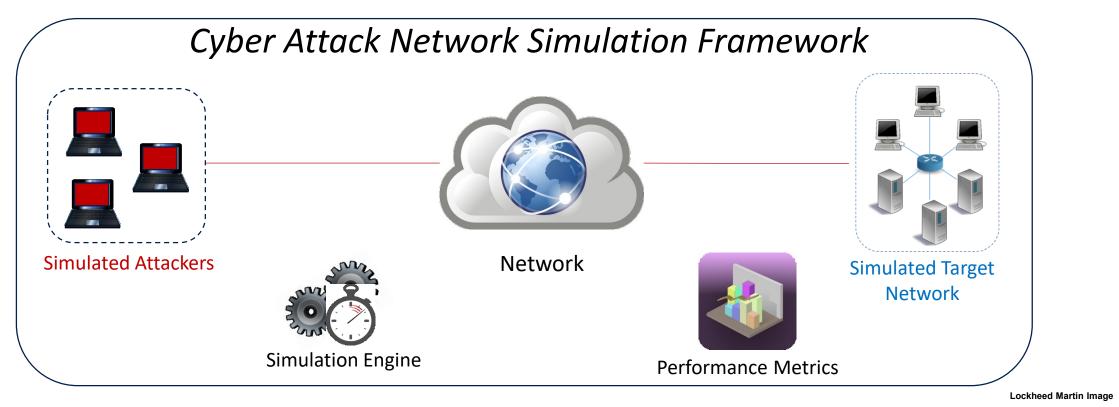
Lockheed Martin Image

### 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.

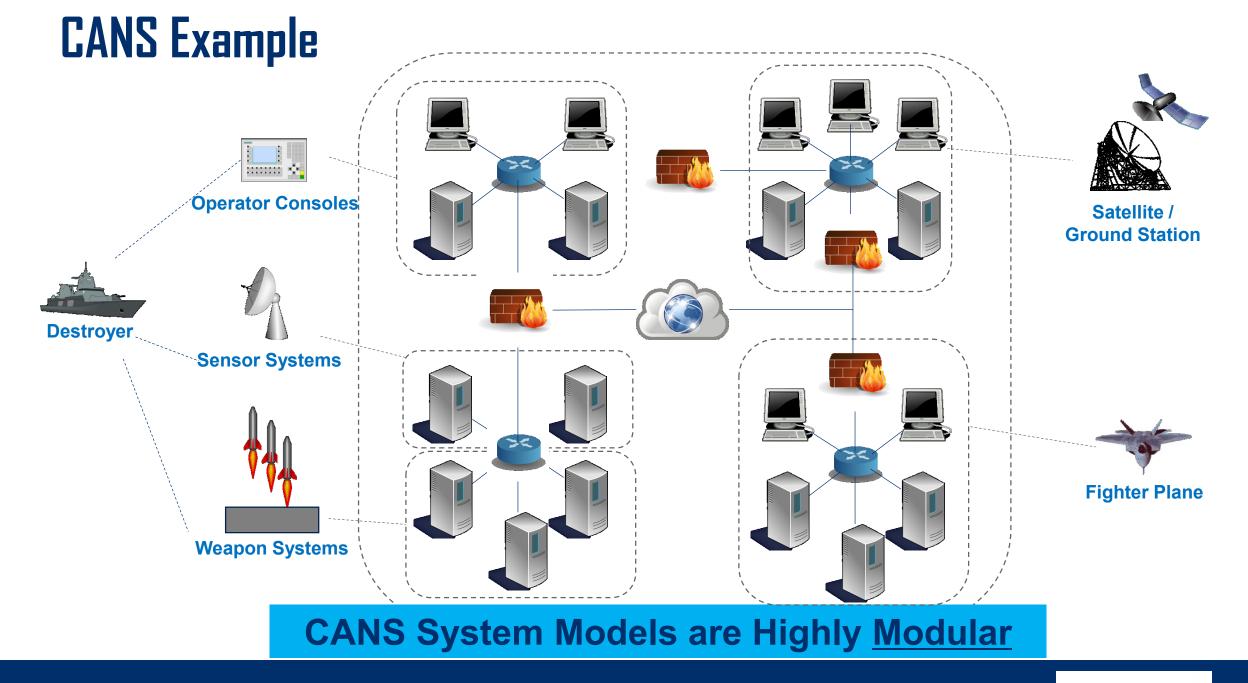
\*Disclaimers: The example shown in this presentation is unclassified; it is not intended to represent any domestic or foreign systems/platforms.

## What is Cyber Attack Network Simulation (CANS)?



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



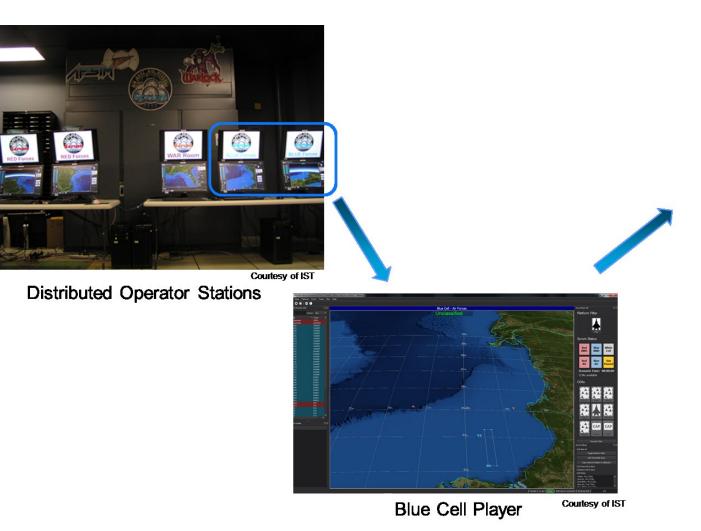
#### What is **AFSIM**?

- 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**



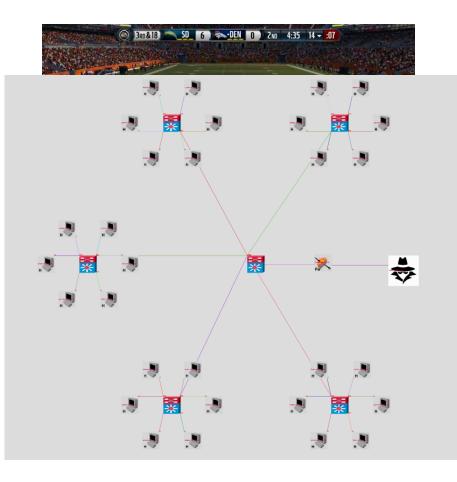
| Q CANS PDU - Warlock |                          |  | ?       | ×  |
|----------------------|--------------------------|--|---------|----|
| Cyber Attack Type:   | 0 - Sensor Turn On (All) |  |         |    |
| Originating Entity:  |                          |  | Set     |    |
| Target Entity:       |                          |  | Set     |    |
|                      |                          |  | Send Pl | DU |

| CANS PDU - Warlock                    |                                      | ? ×      |
|---------------------------------------|--------------------------------------|----------|
| Cyber Attack Type:                    | 0 - Sensor Turn On (All)             | 1        |
| Originating Entity:<br>Target Entity: | 1 - Sensor Turn Off (All)            | Set      |
|                                       | 2 - Comm Turn On (All)               |          |
|                                       | 3 - Comm Turn Off (All)              | Set      |
|                                       | 4 - Weapon Turn On (All)             | Send PDU |
|                                       | 5 - Weapon Turn Off (All)            |          |
|                                       | 6 - Track Mgr Turn On (All)          |          |
|                                       | 7 - Track Mgr Turn Off (All)         |          |
|                                       | 8 - Platform Turn On All Components  |          |
|                                       | 9 - Platform Turn Off All Components |          |
|                                       | 10 - Sensor Spoof (All Tracks)       |          |
|                                       | 11 - Weapon Firing Delay Increase    |          |
|                                       | 12 - Track Mgr Purge All Tracks      |          |

CANS/AFSIM DIS

Lockheed Martin Image

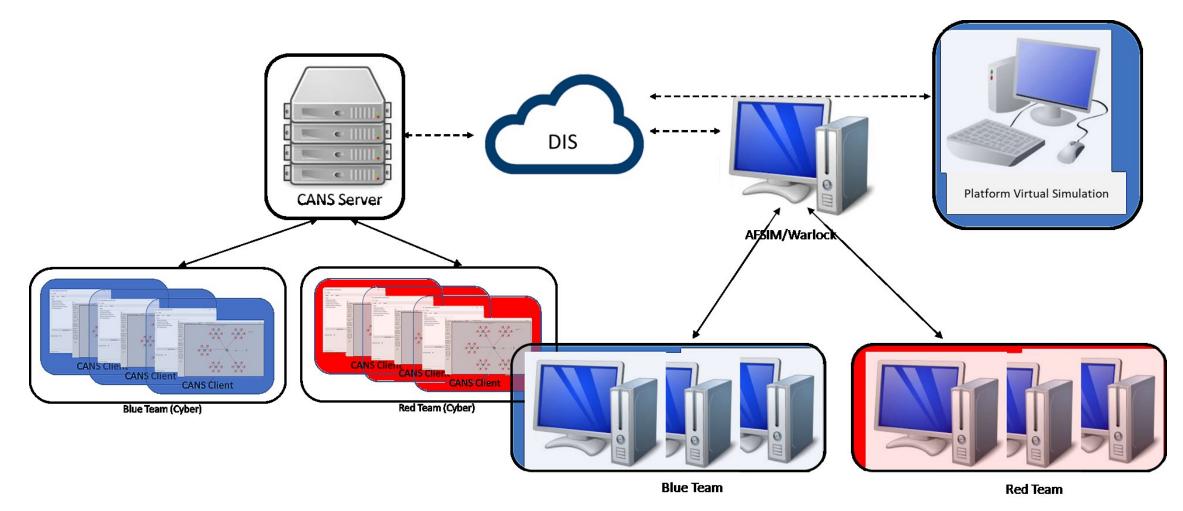
### **EW/Cyber Wargaming**: **A Madden Football Analogy**



| Denial Charlie<br>Denial Bravo<br>Denial Alpha<br>Ping Flood<br>SYN Flood<br>Packet Flood<br>Crash Software<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>Irojan Crnd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>Coovered Notes  | 11 -                 | V/                     | S Corner Roll 2  |
|--|----------------------|------------------------|--|
| Arto       Game       Warr         Sector       CapeC       System Bifo Controls Software       Social Data Encryption System         Account Lockott       Max       Max       State       State         Disable Scatury Software       Disable Scatury Software       Max       State       State         Disable Scatury Software       Disable Scatury Software       Max       Max       State       State         Disable Scatury Software       Disable Scatury Software       Max       Max       Max       State       St   | 🔳 cal                | – 🗆 X                  | 的日本为10%%的0%%%%%的1%的1%%%%%%%%%%%%%%%%%%%%%%%                            |
| Image:  |                      |                        |  |
| > b10       opped       opped <td< td=""><td>Action Queue History</td><td></td><td></td></td<>   | Action Queue History |                        |  |
| billo billo cape: billo cape: billo cape: billo cape: billo billo cape: billo bi   |                      |                        | System Info Controls Software IA Tools Interfaces IDS IDS Filter Ports |
| Visit       Baba         Cisco Cache Replace       Asterned         Visit Asterned       Asterned         Myriad Escape Characters       Disable Fondet         Disable Fondet       Baba         Denial Fondot       Brand         Ponial Charlie       Brand         Denial Alpha       Ping Flood         SYN Flood       Software         Packet Flood       Software         Crash Microsoft Office       Mark         Crash Microsoft Office       Mark         Gain Physical Access       SS         SHP polit       Subvert         Vuert       Subvert  |                      | Target Port 90         |  |
| Cicco Cache Replace<br>Account Lockout<br>Myriad Escape Characters<br>Disable Teinet<br>Disable Teinet<br>Disable Security Software<br>Denial Echo<br>Denial Echo<br>Denial Charlie<br>Denial Bravo<br>Denial Apha<br>Ping Flood<br>SYNF Flood<br>Running<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH A Agent Exploit<br>Subvert<br>Locenet Microsoft Office<br>Chark Transfer Buffer Overflow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lockow<br>Lo | > capec              | Target Address 0.0.0.0 |  |
| Account Lockout<br>Myriad Escape Characters<br>Disable Tenet<br>Disable Seturity Software<br>Denial Echo<br>Denial Charlie<br>Denial Charlie<br>Denial Charlie<br>Denial Alpha<br>Ping Flood<br>SYN Flood<br>Packet Flood<br>Crash Microsoft Office<br>Chunk Trasfer Buffer Overflow<br>* recom<br>* u<br>Topic Craft Software<br>Chunk Trasfer Buffer Overflow<br>* recom<br>* u<br>Topic Chartes Flood<br>System Info Controls Software [La Tools Interfaces IDS IDS Filter, Ports]<br>* recom<br>* u<br>Topic Craft Software<br>Chunk Trasfer Buffer Overflow<br>* recom<br>* u<br>Topic Chunk Trasfer Buffer Overflow<br>* recom<br>* u<br>Topic Churk Trasfer Buffer Overflow<br>* recom<br>* u<br>Topic Churk Trasfer Buffer Overflow<br>* recom<br>* recom<br>* u<br>Topic Churk Trasfer Buffer Overflow<br>* recom<br>* recom<br>* u<br>Topic Churk Trasfer Buffer Overflow<br>* recom<br>* re   |                      | Target Address End     | Stopped Data Encryption System   |
| Mexical Eccopic   Mixing Eccape Characters   Disable Target   Disable Target   Disable Target   Disable Security Software   Denial Charlie   Denial Alpha   Ping Flood   SYN Flood   Packet Flood   Crash Microsoft Office   Churk Tarsfer Buffer Overflow   * recon   Trojan Cmd-Esflitrate Files   Gain Physical Access   SSH Agent Exploit   Subvert  |                      | Al IPs                 | Running Virus Detection  |
| Disable Teinet Disable Teinet Disable Scurity Software Denial Foxtrot Denial Charle Denial Bravo Denial Alpha Pring Flood SYNF Flood Packet Flood Crash Software Crash Microsoft Office Chunk Transfer Buffer Overflow Protocol: Surver B: S   |                      |                        |  |
| Disable Target   Disable Target   Denial Footnot   Denial Charlie   Denial Stravo   Denial Alpha   Ping Flood   SYN Flood   Packet Flood   Crash Microsoft Office   Chunk Transfer Buffer Overflow   > recon   v ua   Tojan Cmd-£xfiltrate Files   Gain Physical Access   SSH Agent Exploit   Subvert  |                      | Source IP Addr 0.0.0.0 |  |
| Disable Security Software<br>Denial Foxtort<br>Denial Echo<br>Denial Delta<br>Denial Chaflie<br>Denial Alpha<br>Ping Flood<br>SYNF Flood<br>Packet Flood<br>Crash Software<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>> recon<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>Deserved Huter   |                      |                        |  |
| Denial Foxtrot<br>Denial Delta<br>Denial Delta<br>Denial Charlie<br>Denial Alpha<br>Ping Flood<br>SYN Flood<br>Packet Flood<br>Crash Software<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>> recon<br>> ua<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>  |                      |                        |  |
| Denial Chafile Denial Chafile Denial Alpha Ping Flood System Info Controls Software IA Tools Interfaces IDS IDS Filter Ports System Info Controls Software IA Tools Interfaces IDS IDS Filter Ports System Info Controls Software IA Tools Interfaces IDS IDS Filter Ports Crash Microsoft Office Chuck Transfer Buffer Overflow recon Low Source IP: Low   |                      |                        |  |
| Denial Charlie Denial Ravo Denial Apha Ping Flood SYN Flood Packet Flood Crash Software Crash Microsoft Office Chunk Transfer Buffer Overflow recon Ua Togin Crnd-Exfiltrate Files Gain Physical Access SSH Agent Exploit Subvert Descrete Neds  |                      |                        |  |
| Denial Bravo<br>Denial Alpha<br>Pring Flood<br>SYN Flood<br>Packet Flood<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>recon<br>• ua<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>• UDOW<br>Course Made  | Denial Delta         |                        | Running Install Uninstall  |
| Denial Alpha<br>Pring Flood<br>SYN Flood<br>Packet Flood<br>Crash Software<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>Concerned Note:<br>Subvert<br>Concerned Note:<br>Subvert<br>Concerned Note:<br>Concerned Note:<br>Subvert<br>Concerned Note:<br>Priority:<br>Subvert<br>Concerned Note:<br>Software (IA Tools Interfaces (IDS) (IDS Filter) Ports<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>Subvert<br>Concerned Note:<br>Software (IA Tools Interfaces (IDS) (IDS Filter) Ports<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:<br>Software (IA Tools Interfaces (IDS) (IDS Filter) Ports<br>Software (IA Tools Interfaces (IDS) (IDS Filter) Ports<br>O HIGH<br>Priority:<br>O HIGH<br>Priority:   | Denial Charlie       |                        |  |
| Ping Flood   SYN Flood   Packet Flood   Crash Software   Crash Microsoft Office   Chunk Transfer Buffer Overflow   recon   ua   Trojan Cmd-£xfiltrate Files   Gain Physical Access   SSH Agent Exploit   Subvert    Port:  |                      |                        | Close  |
| SYN Flood<br>Packet Flood<br>Crash Software<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>> recon<br>V ua<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>V   |                      |                        |  |
| Packet Flood<br>Crash Software<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>> recon<br>> ua<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>> Decovered Nodes<br>Close   |                      |                        |  |
| Crash Software<br>Crash Microsoft Office<br>Chunk Transfer Buffer Overflow<br>> recon<br>* ua<br>Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert<br>Desconverd Nodes<br>Conserver Conserver  |                      |                        |  |
| Crash Microsoft Office Chunk Transfer Buffer Overflow recon ua Trojan Cmd-Exfiltrate Files Gain Physical Access SSH Agent Exploit Subvert Decoverd Nodes Close   |                      |                        | O MEDION   |
| Chunk Transfer Buffer Overflow     recon   ua   Trojan Cmd-£xfiltrate Files   Gain Physical Access   SSH Agent Exploit   Subvert     Descovered Nodes     Descovered Nodes     Close   |                      |                        |  |
| > recon Y ua Trojan Cmd-Exfiltrate Files Gain Physical Access SSH Agent Exploit Subvert > Decovered Nodes Close  |                      |                        | Event: *   |
| ✓ ua       Destination IP:       •         Trojan Cmd-£xfiltrate Files       Protocol:       •         Gain Physical Access       SSH Agent Exploit       Port:       •         Subvert       •       •       •         Descovered Nodes       •       •       •   |                      |                        | Source IP: *   |
| Trojan Cmd-Exfiltrate Files<br>Gain Physical Access<br>SSH Agent Exploit<br>Subvert v<br>Decovered Nodes   |                      |                        | Destination IP:  |
| Gain Physical Access<br>SSH Agent Exploit<br>Subvert Subvert State Filter  |                      |                        |  |
| Subvert V Set Filter Close Close   | Gain Physical Access |                        | Protocol: *  |
| Discovered Nodes   | SSH Agent Exploit    |                        | Port: *  |
| Discovered Nodes   | Subvert v            |                        | Set Filter   |
| Discovered Nodes   |                      |                        |  |
| Lockheed Martin Ima  | Discovered Nodes     |                        | Close  |
|  | Connected to NetSm   | 00000                  | Lockheed Martin Image  |

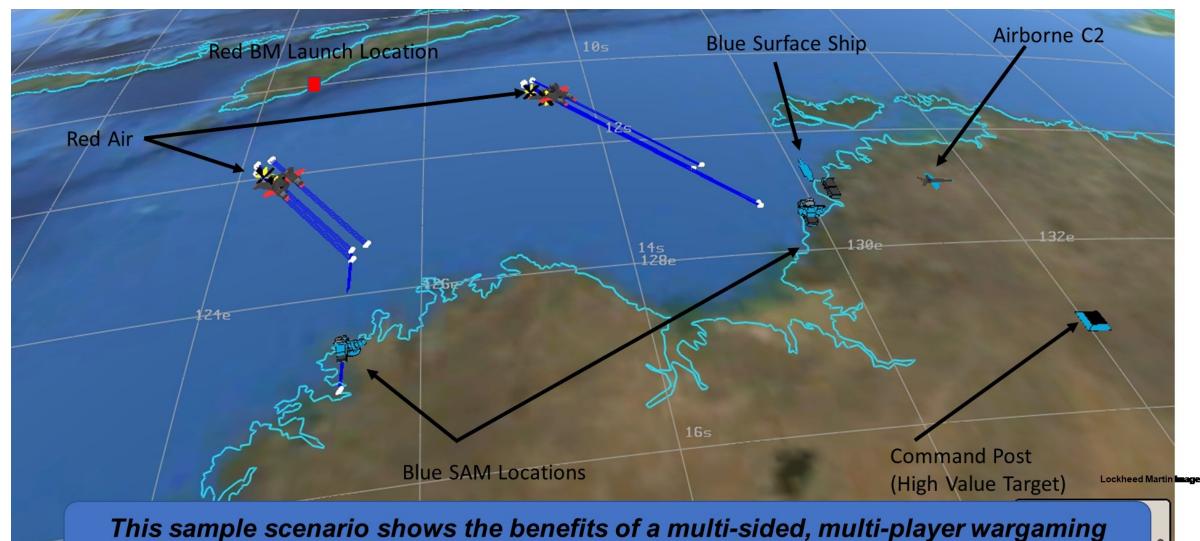
9

#### **CANS/AFSIM Software Architecture**



Lockheed Martin Image

### MDO Scenario OV-1



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?**







Copyright © 2019 Lockheed Martin Corporation