CONNECTIONS 2020

APPLYING AND REPRESENTING A.I./MACHINE LEARNING IN WARGAMING

AUG. 10-14TH

connections-wargaming.com

CONNECTIONS 2020 IS PROUDLY HOSTED BY CNA (CNA.ORG)

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

An OSD A&S Cyber Initiative

Cyber AWARE – Improving the Efficiency, Effectiveness and Dynamics of Cyber War Games

Connections Wargaming Conference

August 2020

James Curbo – JHU/APL
james.curbo@jhuapl.edu

Cyber AWARE Introduction

- Cyber AWARE (Cyber Assessment Wargame Attack/Response Environment) is a wargame management and cyber situational awareness software suite for multi-player cyber wargames.

- Improves game realism by enabling visualization of player actions and effects
- Enables defenders to inject responses
- Allows the adversary team to dynamically create and inject new attacks during the game
- Tailored views give each stakeholder information needed to keep the game in sync and focused on the game objectives

A Sample War Game Scenario

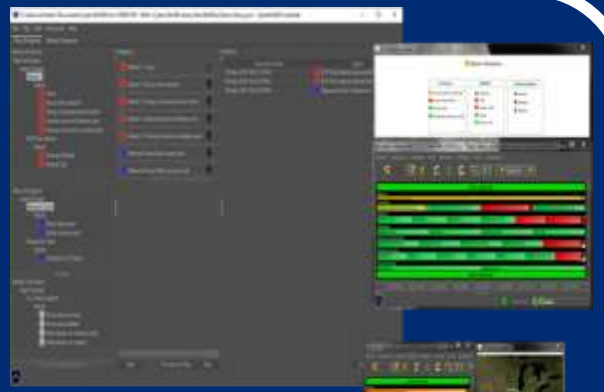
- Game backdrop:
  - The governor of Texas is running for President
  - One of his accomplishments was to promote a system Texas created for families to find each other in a disaster to the federal level
- Red Team:
  - A nation-state adversary does not want the governor elected and is working to undermine him
  - With a hurricane bearing down on Texas, they work to hinder the emergency response of the Texas Emergency Management Agency – EMA
    - Launch a botnet to shut down the “Loved Ones Safe and Well” Website at Emergency Management Agency HQ at the national level
    - Initiate phishing attacks to gain command and control of the Texas office network
    - Use system vulnerabilities to degrade local response in Texas
- Blue Teams:
  - Tactical Blue Team: Texas office network operators and defenders
  - Strategic Blue Team: HQ officials
  - Blue DCO-RA Team: National-level response team

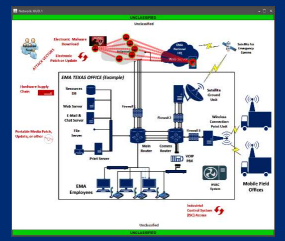
The war game is focused on the procedures between tactical and strategic players and policy questions surrounding the employment of a response team against the adversary

Five Independent Cells – Each Has an Appropriate Coordinated View

White Cell

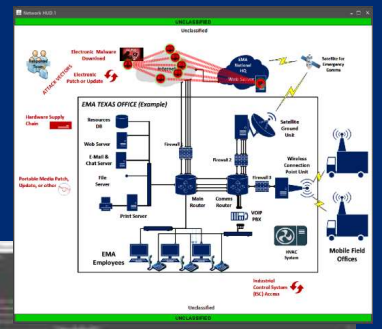
- Coordination
- Adjudication

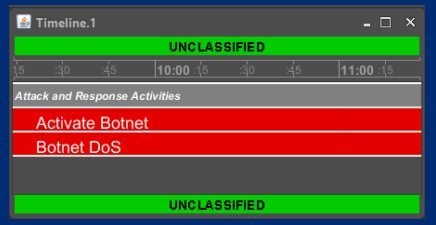




Red Cell

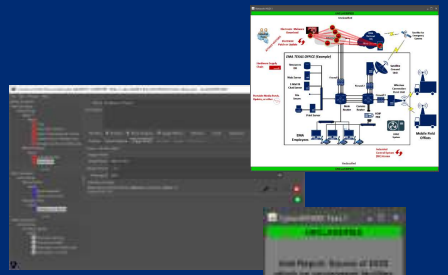
- Attack Plans
- Failure Injection
- Counter Blue Responses





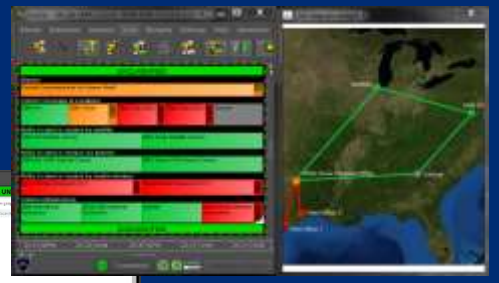
DCO-RA

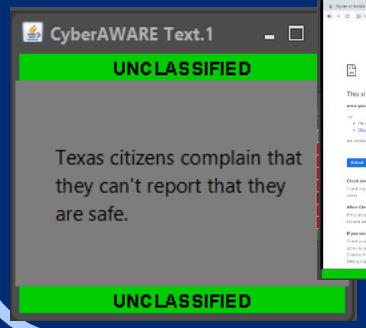
- Red/Gray/Blue space
- Intel reports

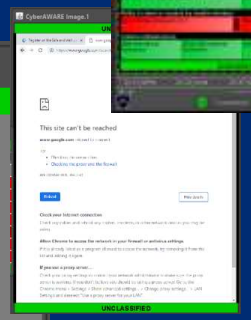


Strategic Blue

- Long View Decisions
- National Assets

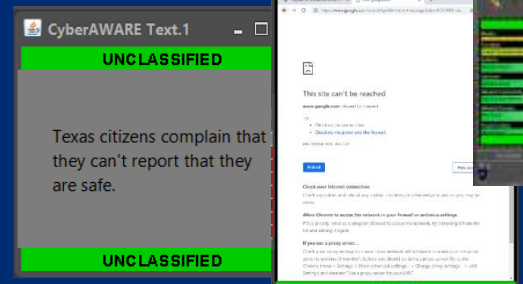






Tactical Blue

- Detect Stimuli
- Propose/Implement Responses



War Gaming Pre-Cyber AWARE

Planning

- Scenario development
- Identification of experts
- Vulnerability workshop
- Attack determination
- Preparation of slides for each cell for each move

Execution

- Introduce the scenario
- Move 1: DOS on national family connection database
- Move 2: Texas office disruption via phishing attack and disruption of local communications

Limitations

Scenarios are planned and played as separate moves.
Move 1 results have no impact on starting point for move 2.

New Approach With Cyber AWARE

Planning

- Scenario development
- Identification of experts
- **Mission dependency analysis**
- Vulnerability workshop
- Attack determination
- **Preparation of planned scenarios in Cyber AWARE**

- Establish an agreed upon model of how the mission and its supporting systems function in advance
- Road-show the model to vet it with experts who can't attend a days-long war game

Execution

- **Brief the mission dependency model**
- Introduce the scenario
- **Maintain synchronized views across cells for shared situational awareness**
- Move 1: DoS on national family connection database
- Move 2: Texas office disruption via phishing attack and disruption of local communications

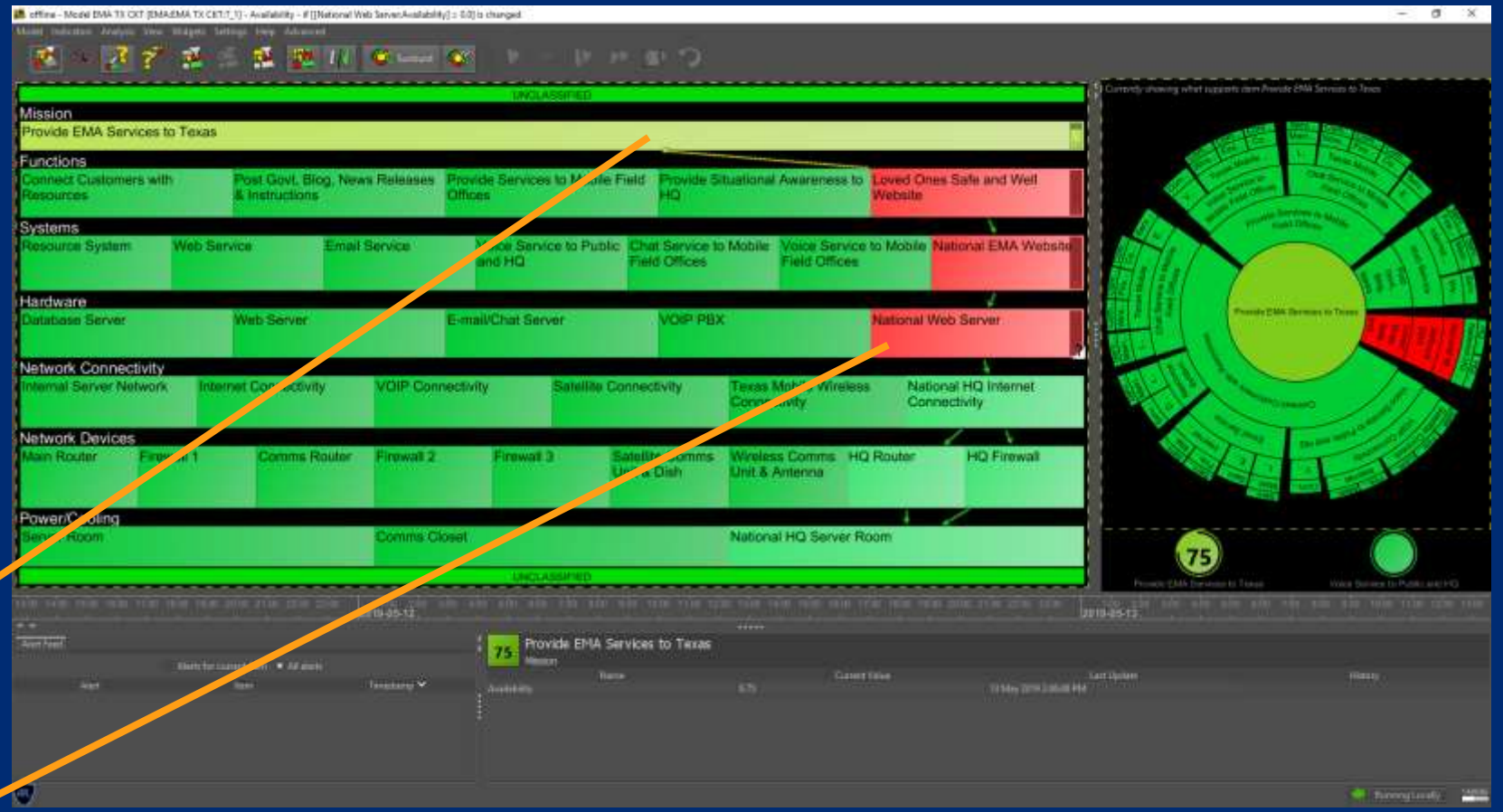
- Brief the participants on the model
- Illustrate how the model results will be communicated in each cell

Observation

Strategic blue cell determines applicability of response team in this scenario.
Blue response to move 1 leads to unexpected modification of move 2.
The mission models provide a better sense of impact at tactical and strategic levels.

Components of Cyber AWARE

- Dagger – Mission dependency modeling capability
  - Used to provide a vetted model of how the system works
  - Embedded formulas dictate how each item's status is calculated
  - Scenario injects show impact to mission
  - Provides calculated mission status information to a variety of displays

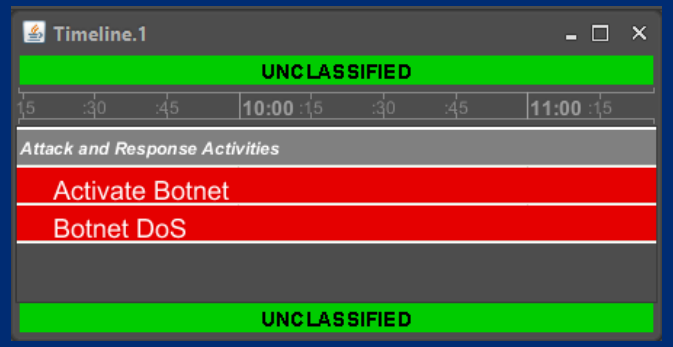


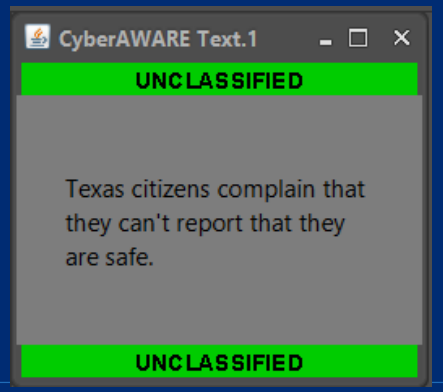
Response Status

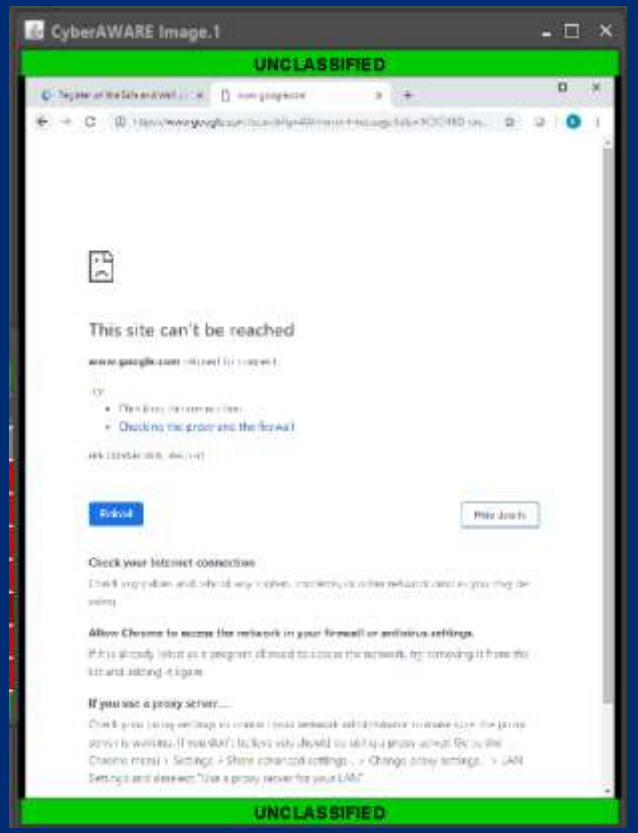
Web Server Status

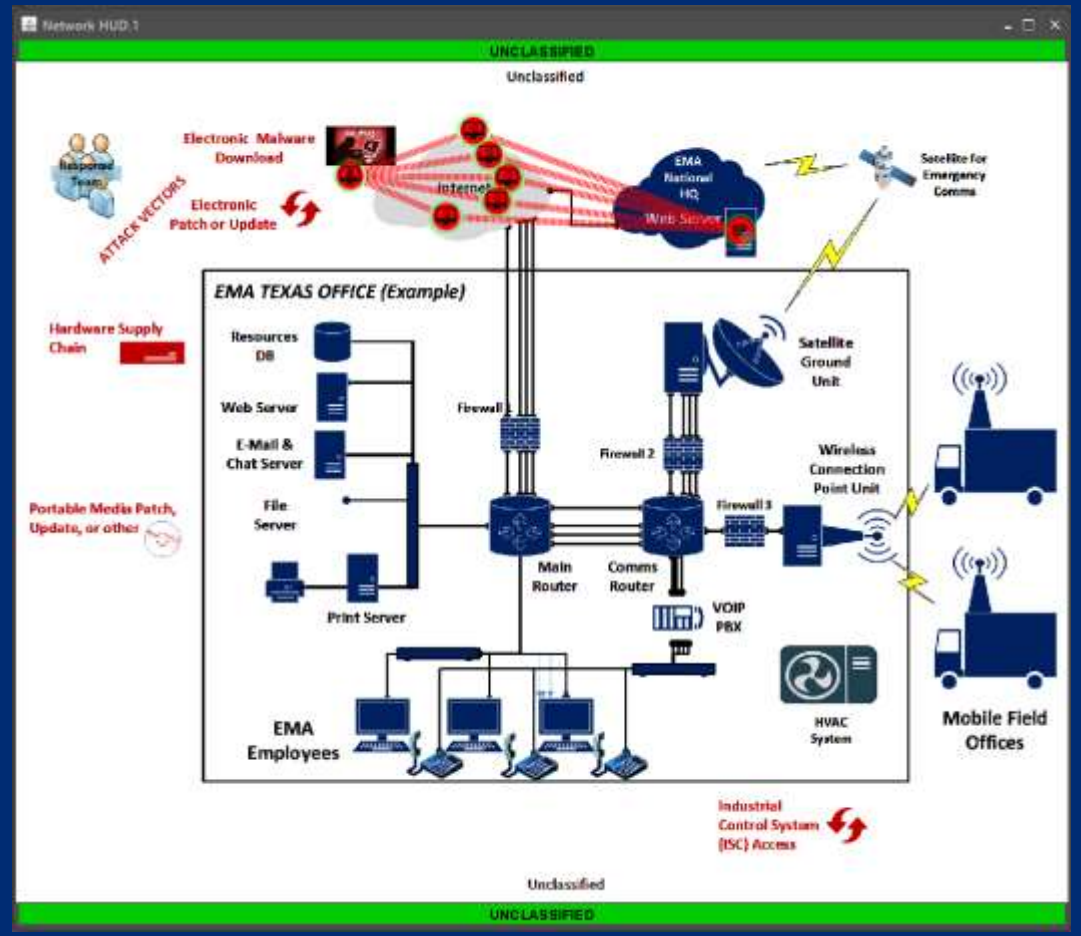
Components of Cyber AWARE

- Treehouse – Shared Situational Awareness Displays
  - Timelines
  - Node-Link Graphs
  - Images
  - Text Messages



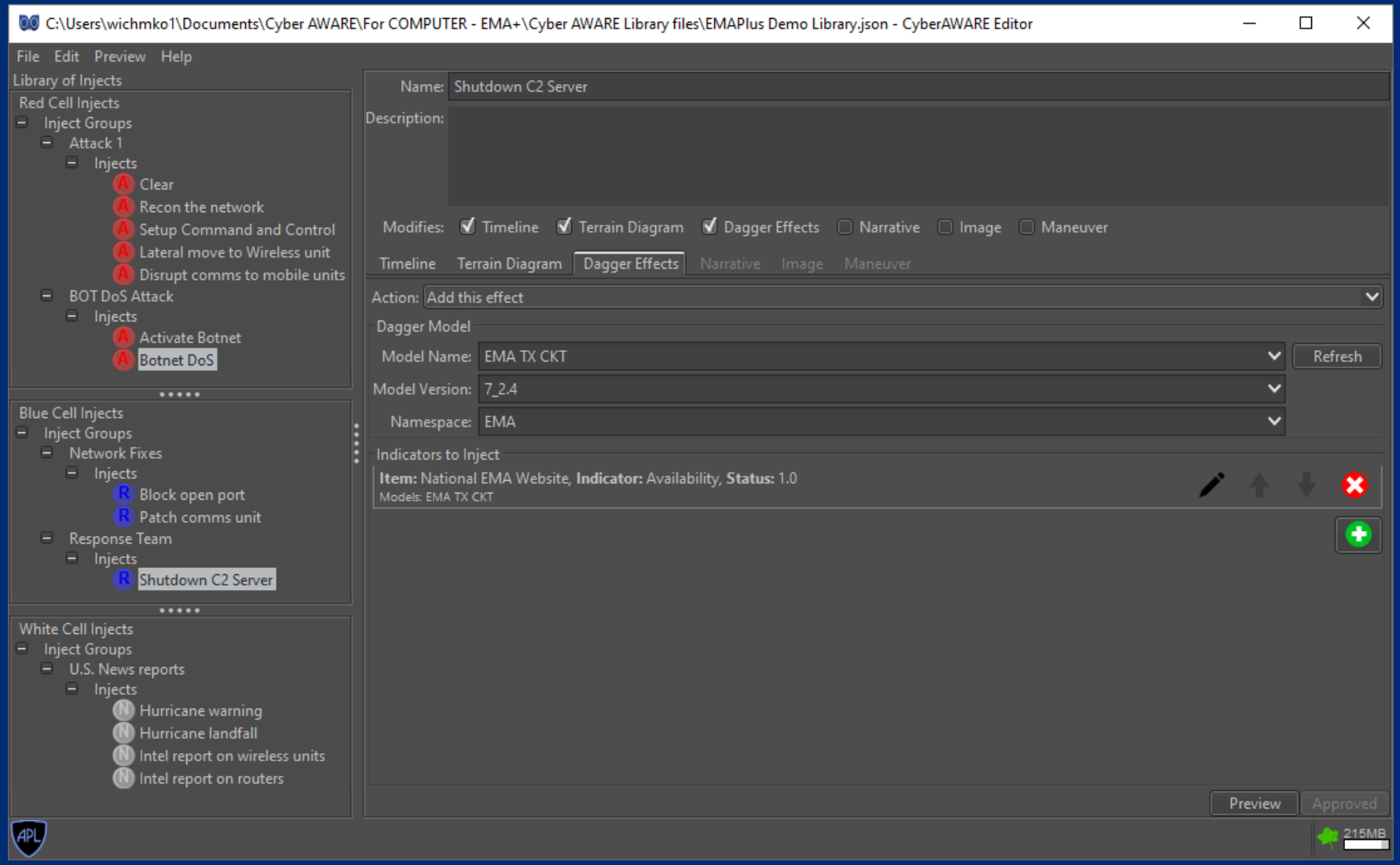






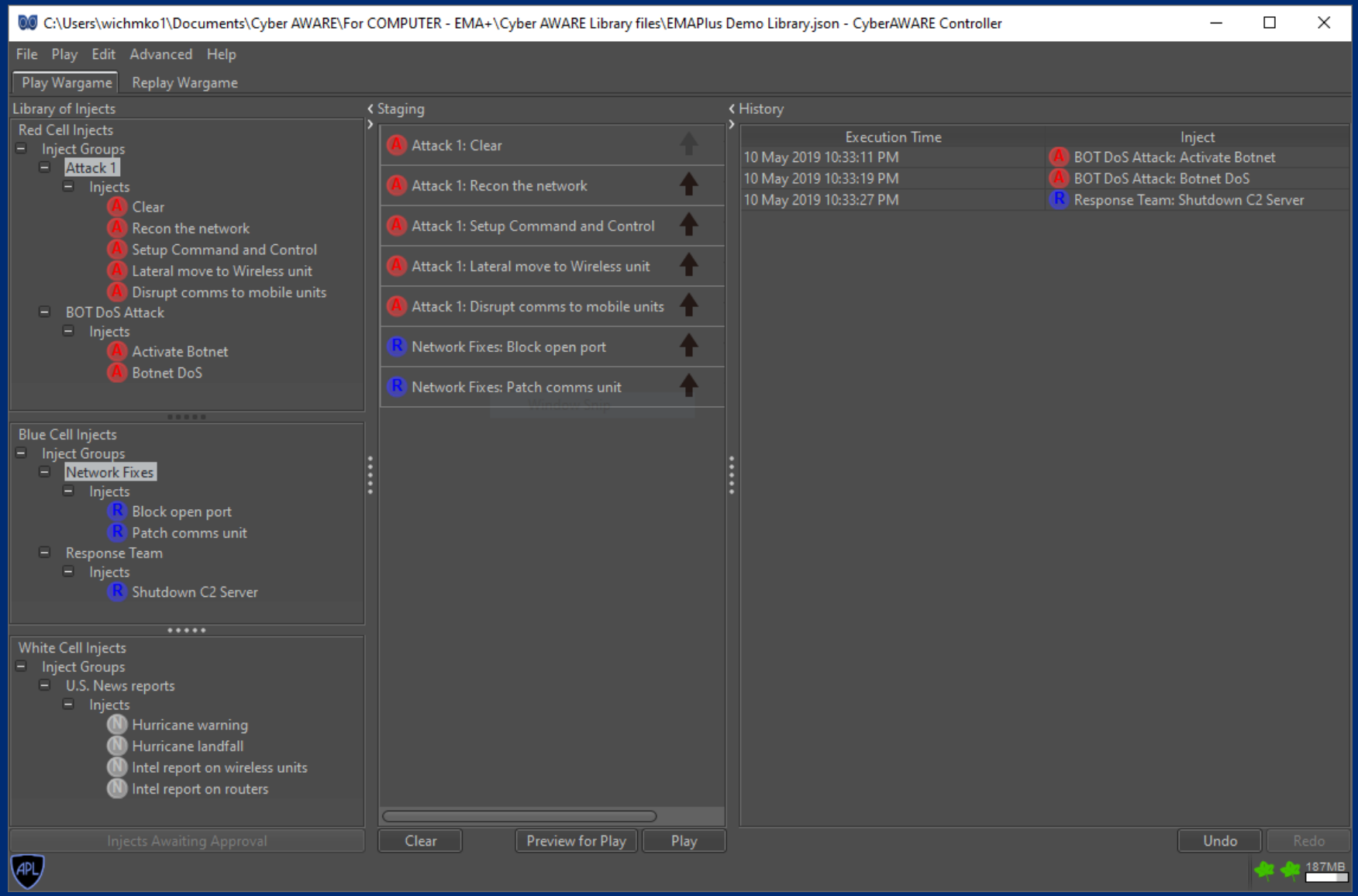
Components of Cyber AWARE

- Cyber AWARE Editor
  - Rapidly defines an inject
  - Defines artifacts for one or more views
    - Timeline, Terrain Diagram, Dagger, Narrative, Image and Maneuver Diagram
  - Supports an approval process



Components of Cyber AWARE

- Cyber AWARE Editor
  - Rapidly defines an inject
  - Defines artifacts for one or more views
    - Timeline, Terrain Diagram, Dagger, Narrative, Image and Maneuver Diagram
  - Supports an approval process
- Cyber AWARE Controller
  - Enables white cell to preview and play planned injects in any order
  - One or more injects can be scheduled and played as a sequence
  - Can call up the editor to create new injects



Cyber AWARE Advances

- All cells are kept in sync with white cell regarding presented materials
- The mission dependency models provide bounds
- Unanticipated blue cell responses can be injected quickly
- Red cell can inject new attacks or rule out next steps based on blue cell choices
- A record of injects played is automatically maintained

Cyber AWARE New and Upcoming Features

- Wartime clock
- Multiple editors so red, blue, DCO-RA injects can be prepped simultaneously
- Finer grained injects based on any Dagger indicator
- Improved human factors
- Improved visualization of chosen actions

Conclusion

- The DoD has been integrating cyber into its TTXs, War Games and Exercises this decade
  - TTXs useful for surfacing considerations, but tend to be static, pre-scripted discussions influenced by the subject matter experts in a single room
  - Large scale exercises can provide rich detail and context, but can be challenging to coordinate the details to genuinely tie network components and packets to operational impact
- OSD A&S Cyber is using war games to focus on the cyber resilience of warfighting systems
  - Multiple cells emulate the separations that exist in the real world
  - The impact of decisions can be determined in a safe environment
- Mission dependency models (via Dagger) are used to enable going beyond system effects to get a Cyber Risk to Mission
- Cyber AWARE enables a synchronized view of effects across multiple cells and the dynamic creation of new injects and responses guided by the bounds of the mission dependency model

Cyber AWARE enhances the quality of player interaction with the scenario and with other players; facilitates telling the Cyber Risk to Mission narrative of the game after the event

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY