Building a Cyber Reference Data Exchange Model for Enabling Cyber M&S Interoperability

Katherine L. Morse, PhD
Principal Professional Staff, JHU/APL
katherine.morse@jhuapl.edu
Need

• Operational Test & Evaluation (OT&E) community has limited capability to incorporate realistic cyber events, attacks, and responses during OT&E events
  - Cyber ranges and cyber models and simulations are not well integrated with live-virtual-constructive test environments

• The lack of integration limits the incorporation of realistic cyberspace conditions into:
  - Major DoD training exercises
  - Test & Evaluation of operational capabilities

• Safe, integrated cyber testing has only been possible for operational systems that can be physically transported into a cyber range.
  - This work is a key step to making realistic cyber representation functional outside of a cyber range.

“The Adversarial Cybersecurity DT&E phase, … , includes an evaluation of the system’s cybersecurity in a mission context, using realistic threat exploitation techniques, while in a representative operating environment.” - The DoD Cybersecurity T&E Guidebook, section 3.3.4, Adversarial Cybersecurity DT&E

“Establish an enterprise-wide cyber modeling and simulation capability. DoD will work in collaboration with the intelligence community to develop the data schema, databases, algorithms, and modeling and simulation (M&S) capabilities necessary to assess the effectiveness of cyber operations.” – The DoD Cyber Strategy, April 2015
Challenge

• We have made significant advances in both cyber M&S and linking models and simulations with cyber ranges.
  - Cyber Operational Architecture Training System (COATS)
  - Analyzing Mission Impacts of Cyber Actions (AMICA)
  - Cyber Operations Battlefield Web Services (COBWebS)
  - Cyber Battlefield Operating Systems Simulation Tools for LVC Simulation (CyberBOSS)
  - Cyber-Argus
  - Joint Non-kinetic Effects Model (JNEM)
  - ...

• The cyber range community came together, through the Cyber Range Interoperability Standards (CRIS) working group to identify keys areas in which the establishment and adoption of standards across cyber ranges will result in efficiencies and improved scalability.

• A similar effort is required to enable the interchange of relevant information between:
  - Cyber ranges and cyber M&S
  - Large exercise training environments
  - OT&E and DT&E environments
Impact

• The highest priority interoperability gap identified by the Cyber M&S Technical Working Group (CyMSTWG) Interoperability Technical Capability Team (ITCT) is the lack of a reference data exchange model (DEM) for cyber.
  - “There is no standard for the exchange of data on cyber attacks, defenses, or effects in the LVC environment.”

• Without the development of a widely accepted Cyber Reference DEM, each federation will define their own to meet their immediate needs.
  - These DEMs will not be interoperable, resulting in the need to modify them and their associated interfaces to achieve broader interoperability in future federations.
Solution

• A standardized and broadly adopted Cyber Reference DEM will be a key contributor to interoperability and reuse within and between cyber and kinetic LVC environments.

• The Cyber Reference DEM will be developed and maintained in an architecture-neutral format with loss-less conversion to multiple architecture-specific formats.
Technical Approach for Prototyping DEM

1. Identify and engage stakeholders, participants, and related efforts [see slides 7 – 8]

2. Develop representative use cases spanning applicable domains [see slides 9 - 12]

3. Determine the scope of the Cyber Reference DEM, e.g., cyber attacks, cyber effects, network representation, offensive and defensive, and sensor reports, based upon use cases

4. Identify content sources that can be leveraged in developing the Cyber Reference DEM [see slides 16 - 19]

5. Develop draft Cyber Reference DEM that meets the defined scope and can be represented in multiple formats, e.g., HLA Evolved FOM, HLA 1.3 FOM, XML messages, TENA LROM, DIS IO PDU, etc.

6. Perform interoperability testing by prototyping application of the Cyber Reference DEM within one or more stakeholder cyber representation and integration capabilities
SISO Cyber M&S Study Group Motivation

• The last several years have seen a significant increase in the number and variety of cyber M&S research and development efforts across government, industry, and academia.

• These efforts have resulted in methodologies and technologies for cyber testing and training that are functionally relevant, but largely independent.

• Broad and deliberate collaboration across these efforts is necessary to meet the rigorous and evolving cyber test and training demands of the defense community.

• The purpose of this study group is to identify key cyber M&S activities, document best practices, highlight lessons learned, and identify areas for potential standardization in order to facilitate adoption by the cyber M&S community.

https://www.sisostds.org/StandardsActivities/StudyGroups.aspx
SISO Cyber M&S Study Group: Organizations Currently Involved

Lead: Katherine L. Morse  JHU/APL
Technical Activity Director: Chris McGroarty  ARL-HRED-STTC

• Primary Proponents:
  – USPACOM J81/ Cyber War Innovation Center (CWIC)
  – US Air National Guard
  – USAF 90th Cyberspace Operations Squadron (COS)
  – Joint Training Integration and Evaluation Center (JTIEC)

• DoD Orgs:
  – Air Force Agency for Modeling & Simulation (AFAMS)
  – Army Research Lab
  – Naval Air Warfare Center Training Systems Division (NAWCTSD)
  – US Army Program Executive Office Simulation Training & Instrumentation (PEO STRI)
  – Office of the Secretary of Defense (OSD) Test Resource Management Center (TRMC)
  – USAF 505th Combat Training Squadron (CTS)
  – US Navy SPAWAR Atlantic

• US Academic /Research Orgs
  – Carnegie Mellon University Software Engineering Institute / Computer Emergency Response Team (CMU SEI/CERT)
  – Johns Hopkins University / Applied Physics Lab (JHU/APL)
  – George Mason University (GMU) C4I/Cyber Center
  – University of Texas  Applied Research Lab (ARL)

• International:
  – Canadian JWFC
  – NATO Joint Force Training Centre (JFTC)
  – MBDA France
  – TNO Defence (The Netherlands)

• Contractor Companies:
  – Alion Science & Technology
  – CACI
  – CapeGemini
  – Dignitas Tech
  – Dynamic Animation Systems
  – Engility Corporation
  – Leidos
  – McGlynn Consulting Group (MCG)
  – Metova
  – SAIC
  – Seajays Consultancy
  – Thales
  – Trideum
Cyber M&S Use Cases

Use Case Template
• Identification
• Goals and MOPs
• Scenario Exemplar
• Conceptual Model
• Potential Components
• DEM Requirements
• Notes, Anomalies, Challenges
• References
• Acronyms

Use Cases To Date
• Mission Effectiveness in a Degraded Environment
• Unmanned Systems Video Degradation Use Case
• Kill Chain in a Degraded Environment
Potential Use Cases (1 & 2 of 5)

- Mission effectiveness in a degraded environment [Testing and Training] (drafted)
  - Attacks executed in a cyber range on an emulation of the operational network; resulting effects passed to an effects emulator in the kinetic simulation environment
    - E.g. COATS
  - DEM requirements:
    1. Target system identification
       - Name or IP address
    2. Target system behavioral effects
       - Effectiveness parameters, e.g. network degradation percent

- Operational test [Testing]
  - Attacks executed in a cyber range on an emulation of the operational network; resulting effects passed to live platforms with embedded emulators on testing range
  - DEM requirements:
    1. Target system identification
       - Name or IP address
    2. Target system behavioral effects
       - Effectiveness parameters, e.g. network degradation percent


Potential Use Cases (3 & 4 of 5)

• Defensive cyber operations [Training]
  - Constructive representation of an attack is passed to a kinetic simulation where its effects are simulated (possibly over time)
    ▪ Attacks may be executed in a cyber range on an emulation of the operational network or they may originate from a constructive cyber simulation in the absence of a cyber range
    ▪ Because the kinetic simulation represents the attack internally, it can model the attack over time
  - DEM requirements:
    1. Target system identification
      ▪ Vulnerable target characterization, e.g. OS, browser, including version #
    2. Attack representation (possibly an enumeration)
      ▪ Attack parameters, e.g. frequency, ports

• Battle staff training in a cyber-contested environment [Training]
  - Attacks executed in a cyber range on an emulation of the operational network; constructive representations of the attacks are passed to kinetic simulations where their effects are simulated (possibly over time)
    ▪ Kinetic simulations could include critical infrastructure and / or SCADA systems
  - DEM requirements:
    1. Target system identification
      ▪ Vulnerable target characterization, e.g. weapons platform, mission command system
    2. Attack representation (possibly an enumeration)
      ▪ Attack parameters, e.g. frequency, ports
Potential Use Case (5 of 5)

- Analysis of OCO / DCO alternatives [Acquisition]
  - Attacks executed in a cyber range on an emulation of the operational network; constructive representations of the attacks are passed to a constructive kinetic simulation environment including a simulation of the system under design with embedded cyber defenses
  - DEM requirements:
    1. Target system identification
       - Name or IP address
    2. Attack representation (possibly an enumeration)
       - Attack parameters, e.g. frequency, ports
Getting Involved

• Subscribe to the Study Group reflector at:
  
  https://discussions.sisostds.org/index.htm?A0=SIW-SG-CYBERMS

• Respond to data calls

• Offer / critique use cases

• Participate in monthly status webcons
Questions?