Introducing Cyber Effects in C2 Simulation

Dr. B. Boltjes[1], Dr. M. Pullen[2], Dr. K. L. Morse[3]

[1]TNO Defence Research, The Netherlands

[2]George Mason University, C4I Centre.

[3]Johns Hopkins University / Applied Physics Laboratory

Top Ten Cyber Effects for Campaign and Mission Simulations

NATO MSG-170, Chair B. Boltjes

MSG: Modelling & Simulation Group

Need

- NATO needs a capability to provide (distributed) mission training for Maritime Air, and Land domains.
- This capability is being developed and has to include C2 systems and new threats such as credible simulation of cyberattacks.

Purpose of MSG-170

- Evaluate and rank the *credibility and likelihood* of the effects in the list
- Categorise at Engineering, Mission and Campaign level
- Gain insight in how simulation of EAC2s can support NATO Cyber Defence efforts
- Invite subject matter experts on the current status of research and best practice on how to achieve/implement effective representations in mission rehearsal and training
- Collect & study “Reference Examples” and/or available implementations
- Consider fidelity levels

Purpose of MSG-170

Key objectives and expected achievements:

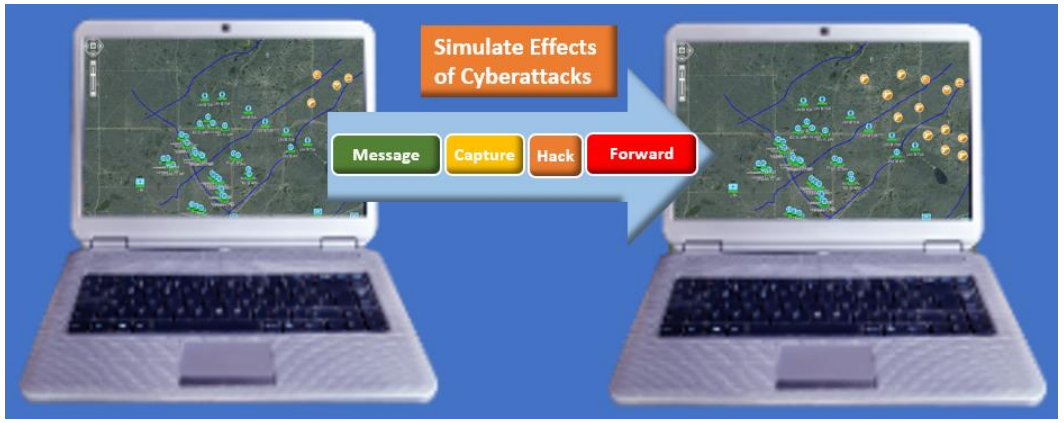
- Produce a “top ten” list of Cyber Effects/Attacks/Countermeasures and Countereffects (EAC2s) that are *most worth modelling*

- Write a MSG technical evaluation report on findings and recommending work for future activities
  - Possibly informing the requirements for a NATO Cyber HLA FOM
  - Consider potential integration with the C2Sim work undertaken by MSGs 048, 085 and 145. (NMSG-151 Presentation by Dr. Mark Pullen, GMU C4I & Cyber Center)

- Dissemination: present on SISO,ITEC, I/ITSEC etc.

SISO: Simulation Interoperability Standards Organization
I/ITSEC: Interservice/ Industry Training, Simulation and Education Conference

Purpose of MSG-170



EAC2s list details:

- Study which elements of the EAC2s are needed in training of processes and procedures for dealing with the cyberattacks .
- Investigate:
  - How to create effective and credible representations and GUI elements for simulation in campaign and mission level exercises of the EAC2s.
  - Current status of research and best practice on how to achieve/implement effective representations in mission rehearsal and training.
  - Ranking method to prioritize list.

Status of MSG-170

- Currently underway

- Technical evaluation report due in August 2019

C2SIM-based Cyber Effects Emulation

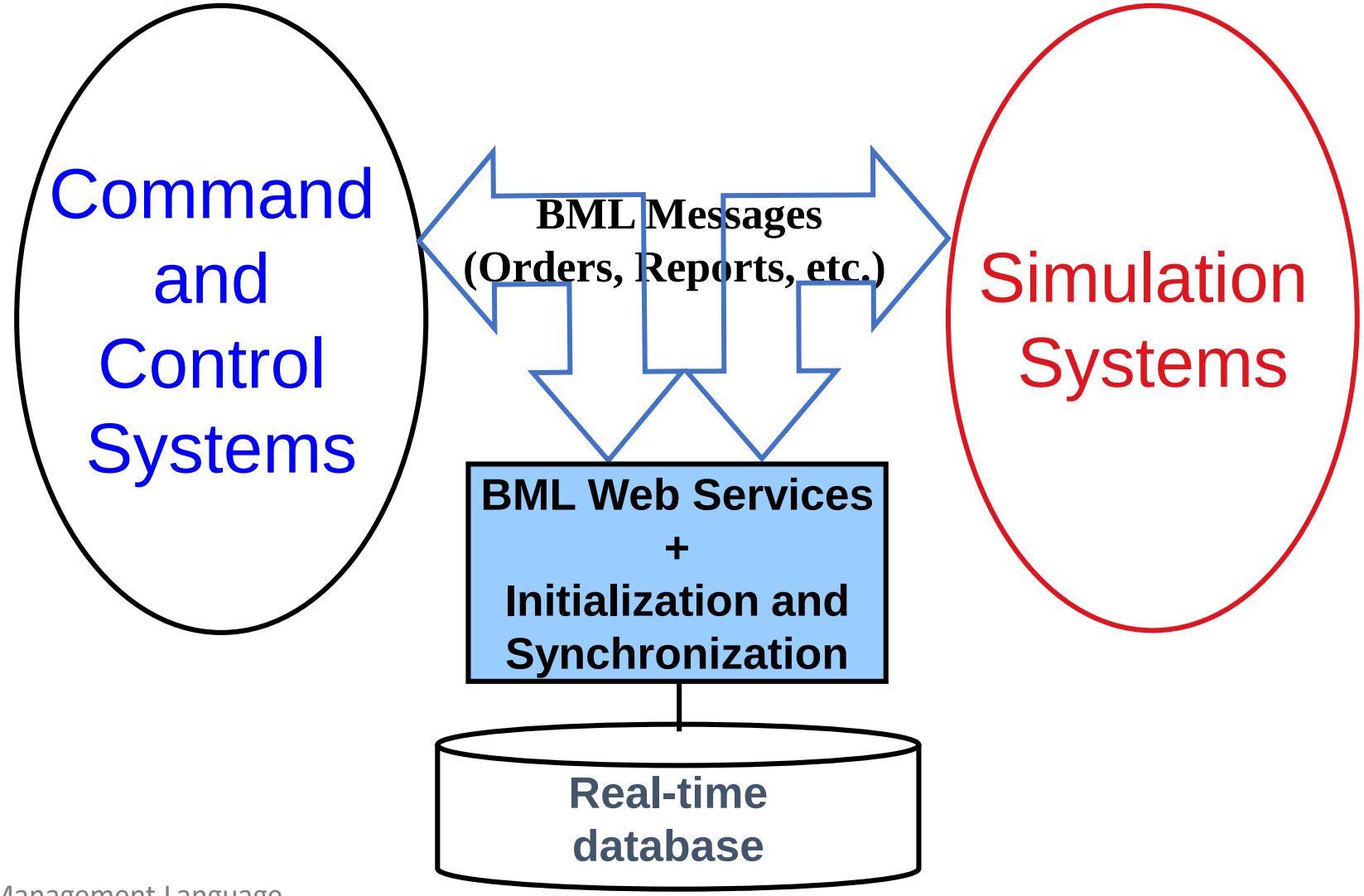
C2SIM Vision

We are working toward a day when the members of a coalition interconnect their networks, command and control (C2) systems, and simulations simply by turning them on and authenticating, in a standards-based environment.

What Does C2SIM Enable

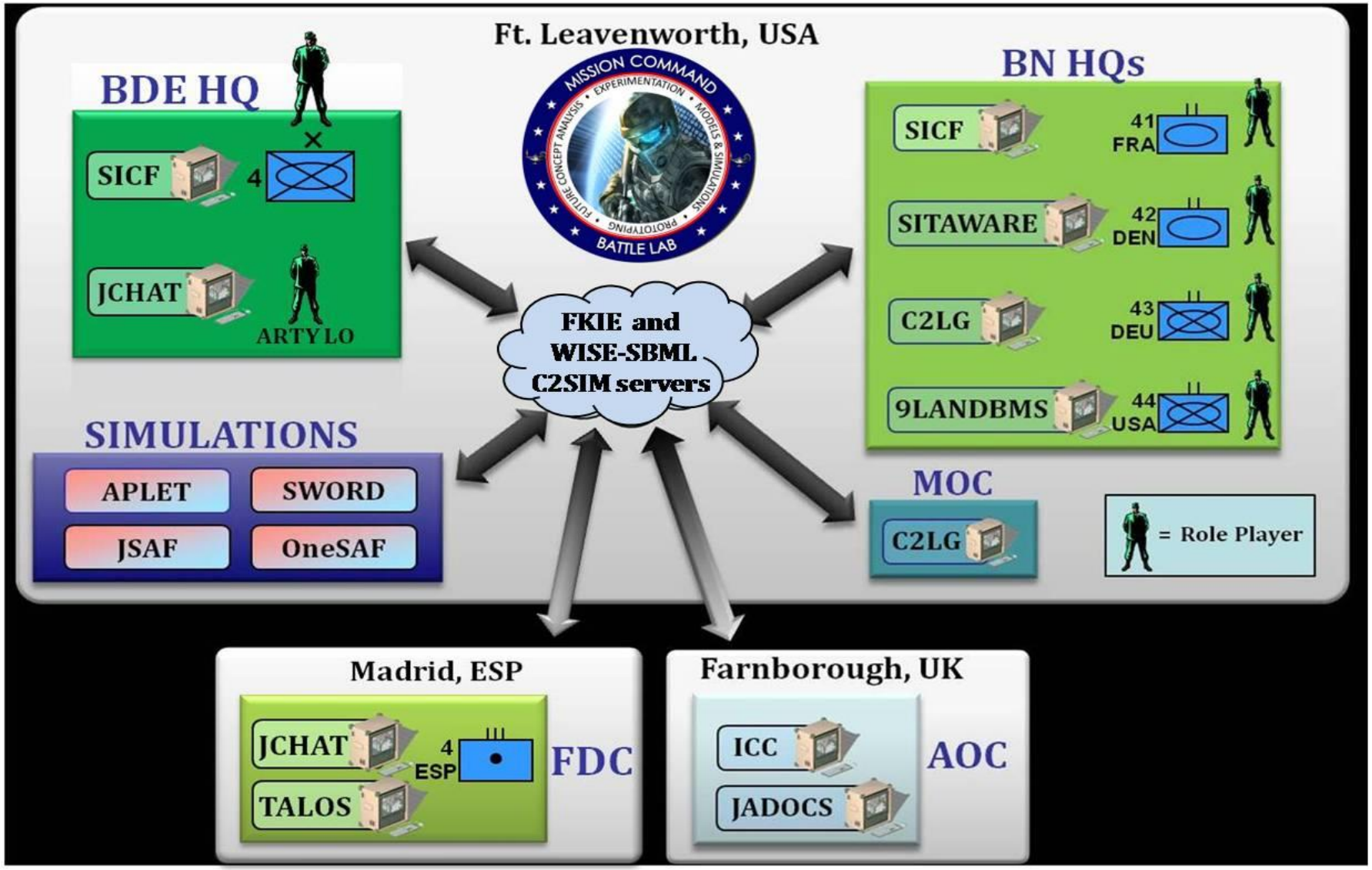
- "Train as you fight"
  - Using operational C2 systems
  - Eliminating human between C2 and simulation systems saves $$$
- Operational planning: COA analysis
- Operational mission rehearsal
- For Service, Joint and Coalition
- Requires cooperative effort of NATO MSG and SISO

C2SIM Basic Architecture



BML: Battlefield Management Language

C2SIM Example:
NATO MSG-085 Final Demonstration Architecture

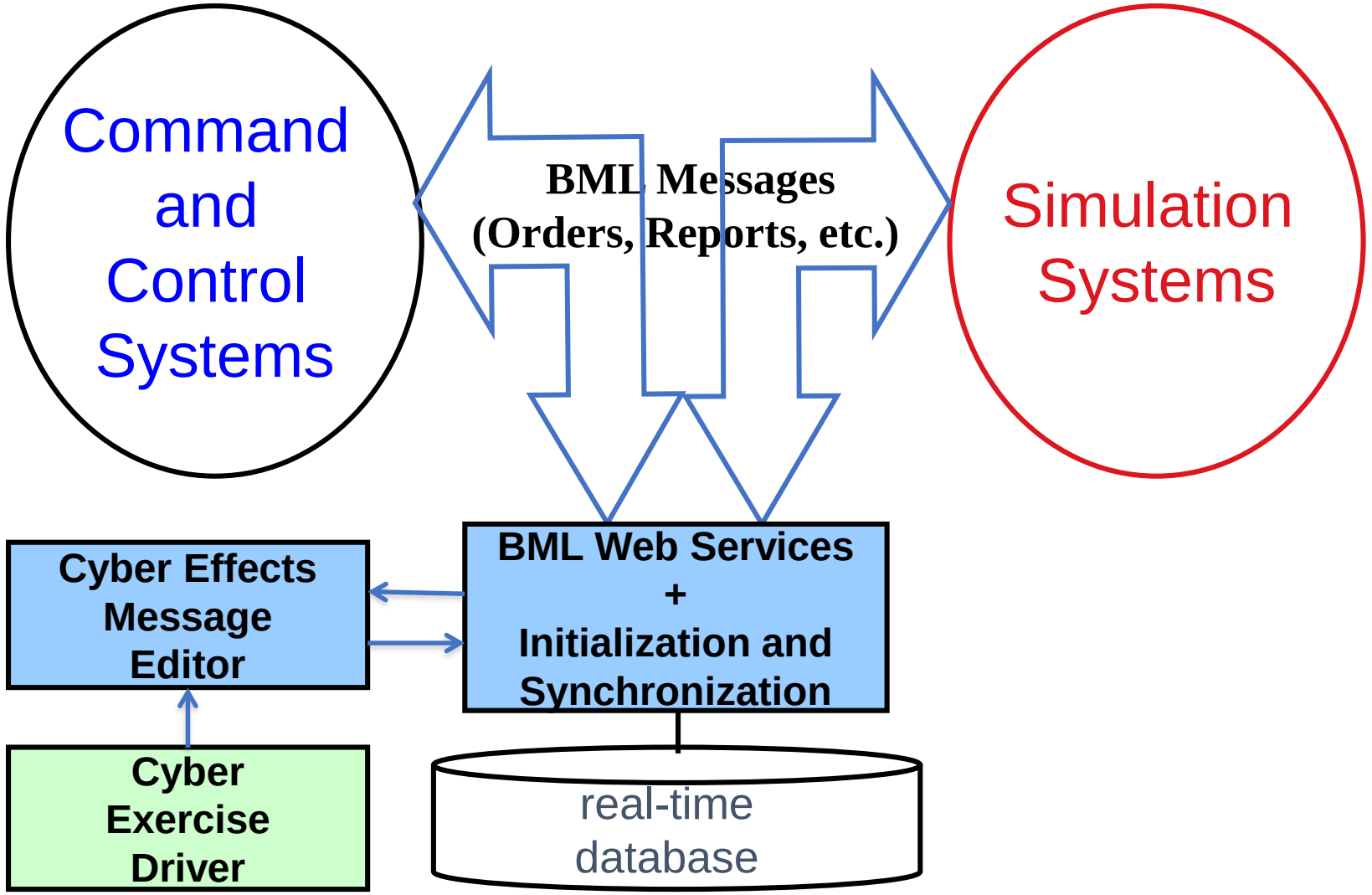


Importance of Training in Cyber-Active Environments

- Two kinds of cybersecurity training:
  - Cyber specialists defending from (attacking?) adversaries
  - Operational military who may have to function under cyber-active conditions
- Second was tested in CWIX 2018 and is critical
  - Forces must not be crippled by cyber attack!
- Concern is for cyber + electronic warfare (CEMA) because impact on operations can be similar
- Actually compromising command and control (C2) would be very disruptive to training exercises
- Modifying the systems so they appear to be compromised is possible but expensive/time-consuming

CWIX: Coalition Warrior Interoperability eXercise

C2SIM Cyber Effects in Operational Training
Expanded C2SIM Architecture



NATO MSG-145 Experimentation, Mini-Exercise and CWIX 2019

- Validating ballotable SISO C2SIM standard
- More complete testing
- Multi-national brigade scenario
- SME role-players debriefed on cyber effects
  - Rounds out C2SIM-Cyber testing from CWIX 2018

SME: Subject Matter Expert

Cyber Reference Data Exchange Model (CyRDEM)

Simulation Interoperability Standards Organization (SISO) Cyber M&S Study Group (SG)

CyRDEM: Cyber Reference Data Exchange Model

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

DT&E: Development Test & Evaluation

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 US DoD 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.

LVC: Live, Virtual & Constructive

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 in SISO

1. Identify and engage stakeholders, participants, and related efforts
2. Develop representative use cases spanning applicable domains
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
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

HLA: High Level Architecture, FOM: Federation Object Model, TENA: Test and Training Enabling Architecture

DIS: Distributed Interactive Simulation, IO PDU: Information Operations Protocol Data Unit

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 Laboratory Simulation and Training Technology Center (STTC)
  - 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

Potential Use Cases (1 & 2 of 5)

- Mission effectiveness in a degraded environment [Testing and Training]
  - 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

OCO/DCO: Offensive Cyber Operations/Defensive Cyber Operations

Getting Involved

- **Subscribe to the Study Group reflector at:**

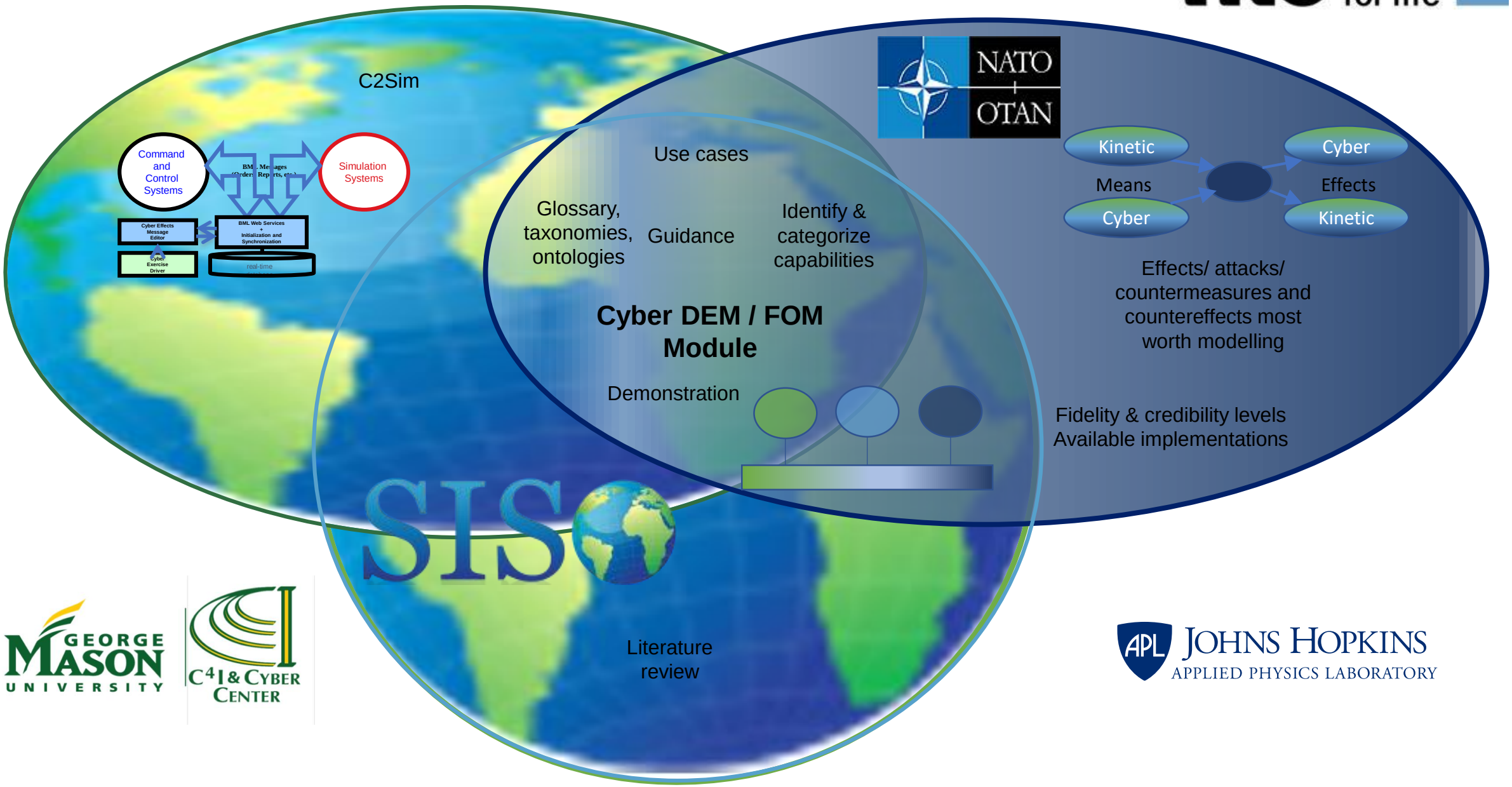
  https://discussions.sisostds.org/index.htm?A0=SIW-SG-CYBERMS

- **Respond to data calls**
- **Offer / critique use cases**
- **Participate in subgroup working meetings**
- **Attend meeting at the SISO SIW conferences:**
  - **https://www.sisostds.org**
- **Follow/Join standardization study/development groups:**
  - **https://www.sisostds.org/StandardsActivities/StudyGroups.aspx**

Common Identified Areas of Work

- Cyber glossary, taxonomies, and ontologies
- Initial NATO Cyber HLA FOM module to exchange simulation information
  - Based upon the SISO Cyber Reference DEM
- Demonstration of cyber M&S capabilities
- Identification of use cases suitable for development
- Reference examples and/or available implementations

Common Identified Areas of Work



Cooperation

- Exchange of knowledge:
  - Existing and standardization efforts and organizations, literature and vendors.
- A large network of researchers in many nations:
    - Defense,
    - Research,
    - Consultancy,
    - Vendors.
- Good mix of expertise:
  - Modelling and simulation (M&S)
  - Cyber
  - Cyber simulation
  - M&S architectures
  - Cyber training
  - Cyber test and evaluation


¿QUESTIONS ?