Cyber Command and Control with CyberBML

Mr. Bo Vargas
Raytheon
4601 North Fairfax Drive
Suite 1200
Arlington, VA 22203
bvargas@hai.com

Outline

- Overview
- CyberBML
- Visualization
- Summary
## Integrated Joint Effects – C2 & NetOps

**Situational Awareness**
- Data fusion to enterprise databases (IA, trouble ticket & MoMs)
- Correlation and root cause analysis
- Known root cause repository
- Real-time and predictive expert analysis
- Service Level Agreements (SLAs)
- End-to-End service management

**Courses of Action**
- CCIRs/IRs
- Mission analysis and mission indicators
- Center of gravity
- Analysis of alternatives
- Modeling and simulation
- War gaming
- Branches & sequels
- Viable options
- Strategic, operational, tactical
- Readiness & availability

**Speed to Command**
- Decision points
- Operational profile
- Running staff estimate
- Enterprise Policy Based Management
- Pre-defined rules of engagement
- Auto-generation of event data, briefs, task orders, NW compliance, battle rhythms, and battle damage assessments
- Operational templates
- Operational capability package
- Non-policy based management

**Effects**
- End State from Commander’s Intent & Purpose
- Kinetic & non-kinetic effects
- Interchangeable/equivalent capabilities
- UJTL, METLs, JCAs
- Measures of effectiveness
- JMEM, JMEM for Cyber
- Nth-order effects assessment
- Electromagnetic spectrum

---

**CyberBML**
Cyber C2/SA with CyberBML

Description


CyberBML Objectives

- Define a capability-based machine-level messaging scheme to communicate mission timelines, tasking assignment, and success/failure of tasks while protecting information at multiple security levels.
- Develop a C2 corpus and natural language processing (NLP) engine to transform unstructured message traffic to reduced corpus structures.
- Define a cyber multi-dimensional cognitive knowledge model, incorporating both structured and unstructured information, for representation of cyber world state, COAs, and plans.
What is this BML?  
(Battle Management Language, developed by GMU)

BML Tasking Grammar

The production rules for basic expressions have the following general form:

\[ B \rightarrow \text{Verb Tasker Taskee (Affected | Action) Where Start-When (End-When) Why Label (Mod)\*} \]

“Where” is a “location phrase”;  
the “When”s are “time phrases”;  
“Why” gives the purpose of the action;  
“Label” is a label given to the task in order allow it to be referred in other basic expressions.
Why Battle Management Language?

- An unambiguous language to:
  - Command and control live and simulated forces conducting military operations, and
  - Provide for situational awareness and a shared, common operational picture
  - Shared semantics between C2 and M&S via a Common Tasking Description
- BML provides an ontology for describing military missions and tasks using C2IEDM.
  - Ontology enables unambiguous “machine instructions”
  - Can be leveraged to input C2 tasking simulations
- The M&S Community requires a standardized approach to C2 Interoperability – BML is a bridge
- Enables rapid M&S-based Course of Action analysis & Information Exchange
- Automated initialization of C2 systems and simulation environments

Unambiguous and machine computable language for M&S

BML Semantic Consistency

BML is being developed as a standard representation of digitized C2 information for executable plans, orders, Requests and reports
- for military units,
- for simulated forces, and
- for future robotic forces.

BML is an Unambiguous Language
- Defined by the role of actionable C2 information
- Provides Unification... across
  - Doctrine and terms
    - Explicit vocabulary and grammar
    - Specific context mapped to operations, scenarios and tasks
  - Conceptual Representation (3 layers)
    - Consistent extension to the C2IEDM
    - Standard framework and exchange model
  - Computational structure
    - Both necessary and sufficient for shared, common understanding
    - Protocols
      - Explicit structure for transmission / sharing

Helps “normalize” Cyber with kinetic warfighting domains
BML History

- **Army BML Development (2001-2003)**
  - Demo of BML Bridge for Brigade/Battalion Operations Order from an NTC Training Mission
  - Used CAPES, an Army C2 System, and OneSAF Army Entity-Level Simulator
  - Complete BML schema in the Joint Common Database (JCDB)

- **XMSF BML Development (2003-2005)**
  - Transferred from JCDB to C2IEDM, Added Web Services
  - Prototyped Air Operations BML including TBMC3 and AWSSIM in Demonstration
  - Moved from OneSAF to JSAF
  - Interfaced to French M&S/C4I system – APPLET
  - Demo to NATO M&S Working Group, Oct 2005

- **geoBML, coalitionBML (2005-2007)**
  - Multinational effort – chaired by US and UK, 8 nations participating in NATO Initiative
  - Terrain Reasoning Capabilities. TEC using BML in its Home Court ATO

- **JBML (2007-2008)**
  - Synchronize service, joint and coalition BML capability development
  - Working with US Army TEC, ODU, Naval Postgraduate School, JNTC Joint Doctrine

- **cyberBML (2008-2009)**
  - Development of new grammar for IA and IO, JC3IEDM extensions for non-kinetic warfare
  - Leveraging JBML Server, JSAF, DMTF CIM Repository
  - Integrated ground and cyber demo simulation in development.

Long history, technical maturity and realistic scenarios

Cyber BML Concept

- Semantically describe the assets, missions and operations for computer network defense (CND), computer network attack (CNA) and computer network exploitation (CNE) that will complement kinetic constructs for joint, multi-domain military operations.
- Provide that model and construct by building upon and extending existing C2 and network schemas and standards: BML and DMTF CIM
- Supports M&S of integrated, joint operations

Platform for M&S of Integrated Operations, including Cyber
Visualization & cyberBML

- Creating “Cyber Battle Management Language”
  - Extending GMU’s Joint Battle Management Language
    - Orders, tasks, reports and requests
    - Using MIT’s M Language
    - Disambiguates definitions, relations
    - Natural language processing
    - Common information model to represent IA in C2 domain
    - Enables correlation & fusion using existing and emerging methods
- Exploring new ways to visualize
  - Rich Internet Applications
  - Mashups of NetOps & C2
  - Web 3.0 interfaces (FLEX)
  - 3D manipulation
  - Natural language markup (future)
  - Spring graphs and tree maps
- Completed trade of security event managers / correlators

Cyber Visualization Environment

- Trends
  - Area/color trending
  - Ontology grouping
  - Zoomable drill-down
- Maps
  - Geo-enabled nodes or semantic parents
  - Link status
- Spring Graph
  - “Roams” ontology–topology & semantic relationships
  - Force-directed auto-layout
  - Details are active data feeds
- Explorer
  - Domain ontology browsing
  - Zoomable
  - Displays object properties
- Window Dock
  - Tool launchers
  - Mac look and feel
  - Set view as background
  - Tile windows
- Charts
  - Time-based scrolling
  - Manipulate, zoom, rotate
  - Tool-tip data detail
- Trends
  - Area/color trending
  - Ontology grouping
  - Zoomable drill-down
- Maps
  - Geo-enabled nodes or semantic parents
  - Link status
- Spring Graph
  - “Roams” ontology–topology & semantic relationships
  - Force-directed auto-layout
  - Details are active data feeds
- Explorer
  - Domain ontology browsing
  - Zoomable
  - Displays object properties
- Window Dock
  - Tool launchers
  - Mac look and feel
  - Set view as background
  - Tile windows
- Charts
  - Time-based scrolling
  - Manipulate, zoom, rotate
  - Tool-tip data detail

Summary

- BML is designed to be unambiguous and machine computable (agent simulations, etc), is normalized with C2 requirements
- cyberBML must be grounded in concepts from CND, CNA, and CNE, but also requires integration with other warfighting domains from a C2 perspective
- Basing both C2 and Network data on open standards opens the aperture for simulations (coalition, not just joint or Army; cross-platform, not just Cisco or PCs).
- High Dimensional Visualizations that combine multiple warfighting domains on the same display, esp. with semantics, offer heightened situational awareness in conjunction with dedicated displays.