A Roadmap to Achieve Cyber Modeling & Simulation Interoperability

Mr. Derek Bryan	**Ingenia Services, Inc.**	**dbryan@ingeniaservices.com**
Dr. David Wells, CMSP	**UCF Institute for Simulation & Training**	**fuzzywells@ist.ucf.edu**
Dr. Katherine L. Morse	**JHU Applied Physics Lab**	**katherine.morse@jhuapl.edu**
Mr. Kevin Hofstra	**By Light Professional IT Services LLC**	**kevin.hofstra@metova.com**
Ms. Sara Meyer	**453rd Electronic Warfare Squadron**	**sara.meyer.1@us.af.mil**
Mr. Jim Ruth	**Trideum Corporation**	**jruth@trideum.com**

ABSTRACT

Cyberspace is a rapidly evolving and contested domain. As a result, government, industry, academia, and international organizations are continuously developing and deploying capabilities to meet the rigorous testing, training and readiness requirements of its users. Ideally these organizations would have conceptual models, validated data, interoperability standards, and other authoritative references to design, build, and employ new capabilities. With this information, organizations could build federated systems-of-systems in an efficient and scalable manner. Without this information, organizations are forced to develop custom solutions that may be incompatible with other solutions and require re-work in the future. This paper will examine the requirements and current state of cyber Modeling and Simulation (M&S) interoperability with a focus on cyber terrain, real-time cyber effects data exchange, cyber-aware interfaces, kinetic and non-kinetic entity correlation, and battle damage assessment. Recommendations will be provided in the form of a candidate roadmap to achieve cyber M&S interoperability. The roadmap will be based on the authors' extensive experience developing kinetic and non-kinetic standards, tools, and systems in support of multi-domain operations training.

ABOUT THE AUTHORS

Derek Bryan is the President of Ingenia Services, Inc. and provides direct support to the Cyber War Innovation Center at U.S. Indo-Pacific Command. He has an M.E. in Modeling and Simulation from Old Dominion University.

Dr. David "Fuzzy" Wells, CMSP is the Deputy Director of the Institute for Simulation & Training at the University of Central Florida. His Ph.D. is in Modeling, Virtual Environments, & Simulation from the Naval Postgraduate School.

Dr. Katherine L. Morse is a Principal Professional Staff member at Johns Hopkins University Applied Physics Laboratory. Her Ph.D. is in Information & Computer Science from the University of California, Irvine. She is the Simulation Interoperability Standards Organization Cyber M&S Study Group lead.

Mr. Kevin Hofstra is the Chief Technology Officer of By Light CyberCENTS. He has a B.S. in Computer Science from Yale University and an M.E. in Telecommunications and an M.E. in Engineering Management from the University of Colorado.

Ms. Sara Meyer is a Computer Scientist at the 453d Electronic Warfare Squadron where she is the LVC lead with M&S software development experience. She holds an M.S. in Information Engineering and Management from SMU.

Mr. Jim Ruth is a Senior Military Analyst at Trideum Corp and the Lead Simulation to Mission Command Interoperability Architect working with Cyberspace and EW M&S. He holds an M.S. in Computer Resources and Information Management.

A Roadmap to Achieve Cyber Modeling & Simulation Interoperability

Mr. Derek Bryan	**Ingenia Services, Inc.**	**dbryan@ingeniaservices.com**
Dr. David Wells, CMSP	**UCF Institute for Simulation & Training**	**fuzzywells@ist.ucf.edu**
Dr. Katherine L. Morse	**JHU Applied Physics Lab**	**katherine.morse@jhuapl.edu**
Mr. Kevin Hofstra	**By Light Professional IT Services LLC**	**kevin.hofstra@metova.com**
Ms. Sara Meyer	**453rd Electronic Warfare Squadron**	**sara.meyer.1@us.af.mil**
Mr. Jim Ruth	**Trideum Corporation**	**jruth@trideum.com**

INTRODUCTION

The demand for greater realism in the representation of cyber operations and effects within training environments in the last decade created a rush of adding cyber warriors onto mission-critical networks during combatant command exercises. Providing true-to-life exposure to cyber threats and operational integration challenges also came with the danger of adversely impacting the training of thousands of participants due to unintended damage and costs caused by live cyber operations. Placing annual operational exercises at risk due to tactical cyber play was clearly not acceptable. Live cyber exercises were moved to isolated sandboxed cyber ranges where simulated representations of red, blue, and gray networks could be attacked, defended, created, manipulated, exploited, and destroyed without real-world consequences. Cyber effects imposed upon the training audience needed to be manageable by a white cell or exercise control group. Emulators were created to safely and securely replicate degraded cyberspace conditions on operational platforms without the use of malware, exploits, or network damage. Simulation developers began to include cyber effects within traditional simulation systems to show the impacts of attacks on their represented entities. What was needed was a method to link cyber range environments, effects emulators, and cyber-aware simulations together to create a holistic cyberspace environment within and between range, simulation and operational enclaves.

As a newly recognized domain of warfare, a cyber data exchange model (DEM) was never incorporated within simulation interoperability standards during the previous decades of standards development and practice. Without a cyber information sharing standard within the simulation community, numerous prototype solutions started to emerge throughout the DoD. The Air Force prototyped a solution based on the Information Operations (IO) Protocol Data Unit (PDU) within the Distributed Interoperability Simulation (DIS) standard (IEEE, 2012). The Army prototyped a Cyber-Kinetic Effects Integration Application Programming Interface based on web services (Guttman, 2017). The Joint community prototyped a cyber DEM (Morse, 2014) based on XML as a component of the Cyber Operational Architecture Training System (Wells, 2015). The quantity and variety of cyber M&S interoperability solutions grew, resulting in methodologies and technologies that were functionally relevant, but largely independent. Broad and deliberate collaboration across these efforts was needed to meet the rigorous and evolving cyber testing and training demands of the defense community. Thus, in early 2018, U.S. Indo-Pacific Command's Cyber War Innovation Center proposed the creation of a Cyber Modeling & Simulation Study Group within the Simulation Interoperability Standards Organization (SISO) 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" (SISO TOR, 2018). The first meeting of the Cyber M&S Study Group occurred at the February 2018 Simulation Innovation Workshop.

The desired end state of this enterprise is an integrated environment that enables real-time information sharing between the cyber domain and the traditional, kinetic domain. Cyber actions and effects that have implications within the traditional kinetic domain must be communicated to and interpreted by the appropriate training audience and systems. Similarly, kinetic actions and effects that have implications within the cyber domain must be communicated to and interpreted by the appropriate cyber audience and systems. The integrated environment will support varying levels of effects including tactical (packet, physical link, node), operational (application, logical link, network), and strategic (system, domain, enterprise). The integrated environment will be compatible with existing best practices and standards for simulation databases, information sharing, simulation management, and after-action review and debriefing, but with appropriate extensions to represent cyber attacks and effects.

This paper introduces the elements of a roadmap for enabling broad and deep interoperability across the DoD with the goal of engaging stakeholders in a constructive conversation to achieve such interoperability.

REQUIRED CAPABILITIES

The following sections describe capabilities needed to meet the vision, requirements, and end state introduced above. Conceptual models and frameworks provide operational context and scope, while real-time data exchange models, data, and tools provide reference implementations to assist capability developers with research, development, test, and evaluation.

Conceptual Models/Frameworks

Conceptual models and frameworks provide an indication of the expansive scope of cyber activities that must be modeled. Most of these are cybersecurity focused, but security focused models do not cover the entire cyber domain. Where there is security, attackers cannot ascertain a cyber persona, nor use cyber or frequency spectrum behaviors as indicators of on-going or upcoming kinetic or non-kinetic activities. Remove cybersecurity and the threat can quickly conduct an analysis of traffic and behavior that allows an estimate of friendly intentions and actions.

The Army Modeling and Simulation (M&S) Office (AMSO) Cyberspace Electromagnetic Activities (CEMA) M&S Framework (CMFW) guides AMSO working group business, especially the identification of "gaps" in M&S and commonality across various projects. The CMFW consists of multiple artifacts that enumerate US Army CEMA doctrine and capture the interrelatedness of various CEMA M&S models for use by Army M&S communities of interest (acquisition, analysis, intelligence, test and evaluation, experimentation, and training). This framework is focused on military operations in cyberspace for the use of M&S to conduct training or analysis of friendly and threat actions. It is currently under development and seeks to connect the non-kinetic, cyber environment with the kinetic environment.

The conceptual models and frameworks noted below are Business Impact Analysis and Enterprise Risk Management focused. These are the two primary perspectives needed to complete an information enterprise analysis (Couretas, 2019). These models support analysis of current networks and behaviors in an effort to mitigate vulnerabilities that would impact freedom of operation.

- Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation privilege (STRIDE) provides a threat model for applications. Threats are mitigated by decomposing your system into relevant components that are then analyzed for susceptibility to each threat. (Herman, 2006)
- MITRE's Adversarial Tactics Techniques & Common Knowledge (ATT&CK™) is a knowledge base of adversary tactics and techniques that provides a foundation to develop specific threat models (https://attack.mitre.org/).
- MITRE's Common Attack Pattern Enumeration and Classification (CAPEC™) provides a comprehensive dictionary of known attack patterns employed by adversaries to exploit known weaknesses in cyber-enabled capabilities (https://capec.mitre.org/).
- NIST Cybersecurity Framework (CSF) consists of standards, guidelines, and best practices to manage cybersecurity-related risk (https://www.nist.gov/cyberframework).
- NIST Special Publication (SP) 800-30, Risk Assessment, is used for baseline cyber system security evaluation (https://www.nist.gov/publications/guide-conducting-risk-assessments).
- MITRE Crown Jewels Analysis (CJA) is a process for identifying those cyber assets that are most critical to the accomplishment of an organization's mission (https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis).
- NIST Risk Management Framework (RMF) provides a process that integrates security and risk management activities into the system development life cycle (https://csrc.nist.gov/Projects/Risk-Management/rmf-overview).
- ISO 3100, Risk Management – Provides principles, framework and a process for managing risk (https://www.iso.org/iso-31000-risk-management.html).

- ISO/IEC 27000 family of standards assists organizations in developing an information security management system (ISMS) to keep information assets secure through a family of standards applied to manage the security of assets (https://www.iso.org/isoiec-27001-information-security.html).
- MITRE's Common Vulnerabilities and Exposures (CVE) contains the list of known information security vulnerabilities and exposures (https://cve.mitre.org).
- NIST National Vulnerability Database (NVD), based on CVE dictionary, is the basis for constructing of attack graphs via know vulnerabilities (https://nvd.nist.gov).
- FIRST's Common Vulnerability Scoring System (CVSS) is an open and standardized vulnerability scoring system (https://www.first.org/cvss/).
- MITRE's Common Weakness Enumeration (CWE) contains a united measurable set of software weaknesses (https://cwe.mitre.org).
- NIST's Common Platform Enumeration (CPE) provides a unified description language for information technology systems (https://nvd.nist.gov/products/cpe).
- NIST's Common Configuration Enumeration (CCE) identifies common system configuration issues (https://nvd.nist.gov/config/cce/index).
- Repository of Industrial Security Incidents (RISI) is a database of industrial controls anomalies to share data across the research community to prevent future cyber anomalies on operational technology (https://www.risidata.com).

Each of the above models and frameworks have their roots in the use of civilian information systems, however they equally apply to the military's cyberspace domain. Cyberspace is a large, complex environment that cannot be segregated into military only operations.

Real-Time Data Exchange Models

A key element to overcoming the current lack of integration is a mechanism that provides a common syntax and semantics for transferring information among kinetic simulations, cyber simulations, and cyber ranges. The requirement for such a Cyber DEM comes from cross-community gaps, and the result must be a cross-community solution. This requirement has been identified in several forums:

- In 2013, JHU/APL performed a study for the Army Operational Test Command (OTC) that identified the need for the Cyber DEM as the second key gap to achieving cyber fair fight in operational test & evaluation, "There is no standard for the exchange of data on cyber attacks, defenses, or effects in the LVC environment."
- The need for a Cyber DEM was the #1 key interoperability gap identified by the Cyber M&S Technical Working Group (CyMSTWG) under the M&S Community of Interest (COI). The CyMSTWG includes membership from operational test & evaluation, training, acquisition, analysis, and cyber ranges.
- "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

Without development of a widely accepted Cyber DEM, each cyber simulation environment will define their own to meet their immediate needs. Their DEMs will not be interoperable, resulting in the need to modify them and their associated interfaces to achieve broader interoperability in future federations. To support the broadest interoperability requirements, the Cyber DEM should be maintained in an architecture-neutral format with loss-less conversion to multiple architecture-specific formats.

A Cyber M&S Study Group (SG) was established under the Simulation Interoperability Standards Organization (SISO). Among other tasks, the Cyber M&S SG is exploring the feasibility of a standardized Cyber DEM. The Cyber DEM is intended to provide the common representation of cyberspace conditions so they can be transmitted bi-directionally among cyber ranges, cyber simulations, and the test / training environments supported by traditional kinetic simulation. This Cyber DEM will be analogous to SISO's Real-Time Platform Reference Federation Object Model (RPR FOM) standard (SISO RPR, 2015). Because it is a standard, the RPR FOM has been broadly adopted for

entity-level, real-time federations. The Cyber M&S SG is executing the following process for developing the Cyber DEM:

1. Identify and engage stakeholders, participants, and related efforts.
2. Develop representative use cases spanning applicable domains. To date, the following use cases have been identified and developed to some level:
    a. Mission Effectiveness in a Degraded Environment
    b. Offensive Cyber Operations Analysis
    c. Cyber Test and Evaluation
    d. Kill Chain in a Degraded Environment
    e. Mission Rehearsal
    f. Battle Staff Training in a Cyber-Contested Environment
    g. Cyber Effects Modeling in a Force-on-Force Simulation Context
    h. Unmanned Systems Video Degradation
    i. Multi-Domain Cyber Training
    j. Information Leakage
    k. Synthetic Cyber Effects for Deployed Headquarters
3. Determine the scope of the Cyber 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 DEM, e.g.
    a. Computer Emergency Response Team Vulnerability Database (https://www.kb.cert.org/vuls/)
    b. CAPEC
    c. ATT&CK
    d. CWE
    e. CVE
    f. Structured Threat Info eXpression (STIX™, https://stixproject.github.io)
    g. Cyber Operation Architecture Training System (COATS) DEM
5. Develop the draft Cyber DEM that meets the defined scope and can be represented in multiple formats, e.g., High Level Architecture (HLA) Evolved FOM, HLA 1.3 FOM, Extensible Markup Language (XML) messages, Test & Training Enabling Architecture (TENA) Logical Range Object Model (LROM), DIS IO PDU, JavaScript Object Notation (JSON).
6. Perform interoperability testing by prototyping application of the Cyber DEM within one or more stakeholder cyber representation and integration capabilities.
7. Decide whether to pursue standardization through SISO.

At this writing, the Cyber M&S SG is focused on steps 3 – 5. The figure below provides a current snapshot of the Cyber DEM in the Unified Modeling Language.

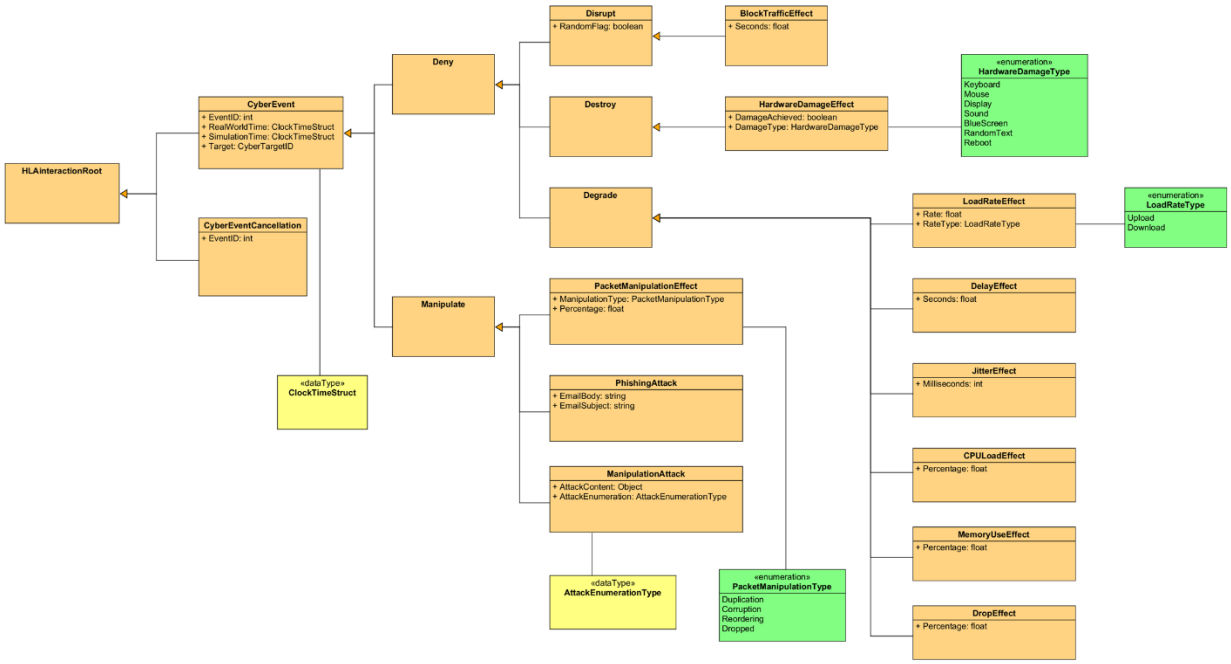

Figure 1: Geddes, A. 2019. *Cyber DEM UML*

The SG expects to complete the first draft of the Cyber DEM in November or December 2019. The results will be included in a final report to be completed in December 2019. If the SG decides to pursue standardization, a product nomination (PN) will be submitted to SISO in January 2020 in anticipation of launching a product development group (PDG) at the 2020 Simulation Innovation Workshop (SIW) in February 2020.

Data

A key driver to kinetic simulation capabilities and fair fight is data. The same is true for the cyber domain. Data is needed to describe cyber key terrain / environment, scenario, vulnerabilities, and damage assessment. While some of these data requirements are under consideration by SISO and other groups, none of these data requirements have been adequately addressed or standardized by the broader cyber M&S community.

Cyber Key Terrain / Environment

The U.S. Army describes key terrain as "any locality or area, the seizure or retention of which affords a marked advantage to either combatant" (FM 3-90-1, 2013). Cyber key terrain refers to the systems and information that are critical to the operational missions. The description of cyber key terrain in multi-domain operations is often characterized through components existing within layered planes (Raymond, 2014):

- Supervisory – C2 operational control components
- Cyber Persona – Identities or individuals
- Logical – OS, applications, relations and logical links
- Physical – Computers, network devices and connection components
- Geographic – Physical location of the system components or logical information

The key terrain / environment characterizes the system and structure that makes up the cyber domain. It defines the entities that exist and how they relate to each other. In the cyber simulation this is generally a network topology for interconnected TCP/IP systems, such as computers, routers, switches and network services. The expression of this data is often represented in a machine-readable format that is referred to as infrastructure as code. The definition includes infrastructure with both virtual and physical machines along with network resources and services. This definition can be managed through a version control system and generally uses scripts or declarative definitions. Examples of cyber environment definitions include text definitions such as YAML (YAML Ain't Markup Language)

or declarative file-based definitions such as terraform. The primary advantages of having a machine-readable cyber environment definition include reusability/interoperability by standard definitions across diverse workspaces, speed due to automation of both changes and execution and also risk reduction by removing the manual processes associated with network deployment.

Cyber Scenario

The scenario defines the injects that occur within the cyber domain during an event. This is a list of master scenario events split into categories of predefined actions such as threat emulation, traffic generation and intelligence injects. Threat campaigns are often defined according to the STIX which is a language and serialization format used to exchange cyber threat intelligence (https://oasis-open.github.io/cti-documentation/stix/intro.html). Traffic models are often represented by JSON formatted representation of sources, destinations, traffic types and pseudo randomized user emulation components. Intelligence injects are scenario-linked information components, such as social media, websites, databases and cyber personas that can be used for collection, analysis and targeting.

Vulnerabilities

Vulnerabilities within the cyber domain are generally categorized through the CVE referenced earlier. This database defines the exposure level associated with publicly known cyber vulnerability using common identifiers to provide a standardized method for describing the vulnerability and referring to the NVD. The NVD then provides the attributes of the vulnerability including the vector, complexity, privileges and scope.

Damage Assessment

In the cyber domain, damage assessment is typically based upon information security attributes of:

- Confidentiality – secrecy or non-disclosure from unauthorized users
- Integrity – accuracy or completeness of data
- Availability – accessibility of resources and data

Damage to a cyber system will generally be categorized in these terms. This relates to some of the kinetic attributes of platforms, for example, a damaged or destroyed system would have degraded availability. However, additional concepts of damage are applied differently for an information resource, such as data, because the confidentiality or integrity can be impacted without any kinetic action.

Tools

Cyber Simulations

Cyber Simulations have a number of common and well-defined elements that categorize the cyber environment. Most specifically a cyber environment can be characterized by two components: cyber terrain (typically referred to as the environment) and cyber events (typically referred to as the scenario). These components can be defined in a set of fundamental building blocks that allow them to be standardized across simulation systems so that the designs are interoperable with each other and data can be exchanged across the systems.

Simulations that model communication networks typically model the nodes that will communicate, the links between those nodes, and the data that is passed over those links. The two categories of links are logical and physical.

A logical link model represents the ability for two sites to communicate without considering the communication backbone. The model considers the link active or inactive, and the model does not care why the state changed.

A physical link model considers the communication backbone, like communication towers or satellites, to examine the multiple paths that the data could traverse over the logical link. Physical link models keep track of the effects that change the state of the link between active and inactive.

In Figure 1, the logical link is between Site A and Site B. Two physical links exist between those nodes because Site A and Site B have the ability to communicate through either Comm Tower 1 or Comm Tower 2. If Comm Tower 1

is destroyed by a kinetic strike, Site A and Site B will still be able to communicate through Comm Tower 2, so the logical link is still active. If both Comm Tower 1 and Comm Tower 2 are destroyed, Site A and Site B will not be able to communicate with each other, so the logical link would be considered inactive.

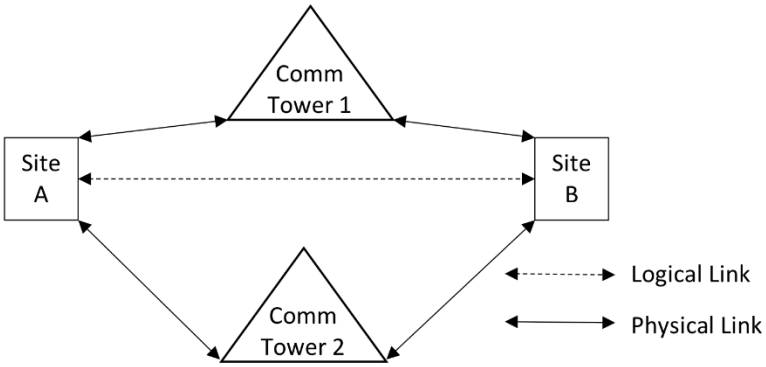

Figure 2: Logical and Physical Link Example

In exercises like Blue Flag, Virtual Flag, and Ulchi Freedom Guardian, logical link models work in conjunction with physical link models to ensure the training audience has a comprehensive picture of the effects from kinetic strikes and cyber attacks. The physical link model adjudicates the results of attacks and passes the results to the logical link model through some form of data exchange like the IO PDU, Federation Object Model (FOM) interaction, or simulation-specific interface. Those data exchange methods are simulation- or exercise-specific and do not offer interoperability throughout the cyber M&S community.

Currently, kinetic simulations are mostly subjected to the comms effects described above which happens externally to the simulation. The next step is to modify kinetic simulations to represent cyber attacks and effects internally which would enable representation of a broader range of attacks and effects, and more subtle ones.

The vulnerability of blue systems to specific attacks is classified. Adding cyber attacks has the potential to change the classification level of a simulation and any event / exercise in which it participates. One solution to this problem is to segregate attack representation and effects determination on the high side (Morse, 2014). One simulation system models the attack on the high side, and the effects are communicated through an interface to another simulation system on the low side where the training audience only sees the effects.

Cyber-Aware Interfaces

Interfaces or gateways are often used to facilitate information sharing between cyber and kinetic simulations for several reasons. Cyber simulations are typically executed on alternate networks due to either classification or risk of exposure. Also, the vast majority of cyber simulations do not implement traditional DoD simulation protocols (e.g., HLA/DIS/TENA). As a result, interfaces that can receive, interpret, and send cyber actions and effects are needed. The USAF created and used a cyber-aware ruleset for Radiant Mercury as part of the COATS project (Wells, 2015) and the U.S. Navy adapted the Joint Simulation Bus to include a cyber plugin to its translator framework for Operation Blended Warrior (Moore, 2018). Additional and more capable cyber-aware interfaces will be needed in the future to ensure interoperability between cyber and kinetic simulation environments.

ROADMAP

The following sections present a roadmap – priorities, processes/steps, opportunities and challenges – to achieve the required capabilities described above.

Priorities

The Cyber DEM will be the glue that holds together the components of cyber M&S interoperability. Its common syntax and semantics for transferring information among kinetic simulations, cyber simulations, and cyber ranges will

enable interoperability and reuse without the need for conversion of representations, an issue that has plagued kinetic simulation for decades. Its completion and standardization are urgent because the need for this type of data exchange is immediate. Without a broadly-accepted standard that meets the needs of the whole community, individual projects and programs will adopt bespoke solutions, practically guaranteeing non-interoperability. Fortunately, there is broad interest and participation in the development of the Cyber DEM.

The Cyber DEM can only achieve its objectives if kinetic simulations are made cyber-aware, making use of the data conveyed in accordance with the DEM. Most effects that can be achieved currently are external to kinetic simulations, e.g. simulating interference with incoming communications. But this represents only a limited set of the effects that can impact operational systems. Just as it's a requirement to represent kinetic effects on operational systems, it should be a requirement to represent cyber effects on them.

Runtime data exchange is not the only cyber data need. Just as kinetic simulations need initialization for unit order of battle, terrain, and scenarios, cyber simulations need electronic order of battle, network and node representations, and cyber scenarios. Standardizing on these data formats will reduce exercise and event set up time by removing the need to convert data between formats, a task that also tends to introduce errors with their attendant impacts. This will also result in increased reusability.

Finally, standardized data storage and exchange formats cannot be effective without actual data. Representative network, node, attack, and effect data is needed to populate and run training, analysis, and experimentation simulations. Actual network, node, attack, and effect data is needed to populate and run testing, analysis, and experimentation simulations. While collection of this latter type of data about blue systems will be very sensitive (and needs to be protected accordingly), it is still critical to understanding and addressing vulnerabilities.

Processes/Steps

Figure 3 below outlines the major proposed processes/steps to achieving long-term cyber M&S interoperability via a community-driven, standards approach. The initial phase, real-time data exchange models, is underway via SISO's Cyber M&S Study Group. This paper outlines pockets of activity in the next two phases, data specifications and interfaces, but these activities are project-driven vice community and standards driven. It would be ideal if a Service or agency led an effort to standardize cyber M&S specifications and interfaces similar to real-time data exchange models. Once the first two phases are complete, reference implementations can be developed, socialized, and matured to assist in capability development across the community. Finally, adoption, standardization, and maintenance of products are conducted to ensure the long-term integrity and sustainability of applicable capabilities.

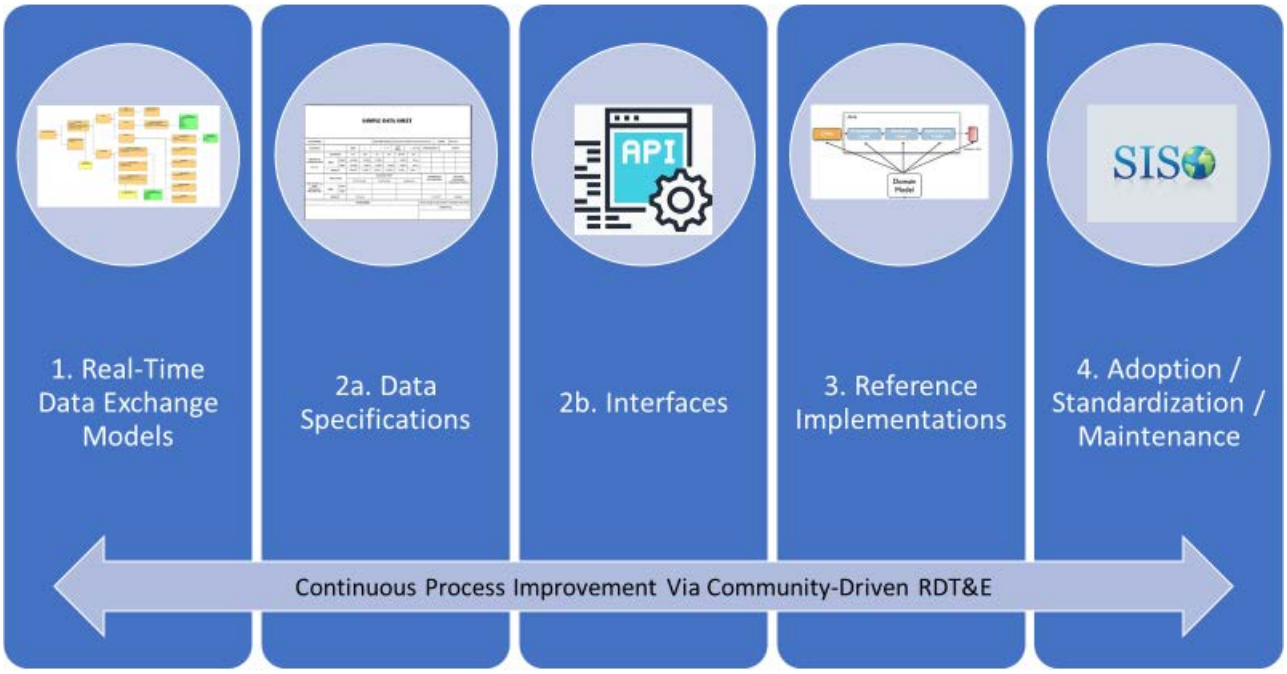

Figure 3: Cyber M&S Interoperability Roadmap

Opportunities and Challenges

Endorsement of the Cyber DEM and other solutions by senior DoD and Service leadership presents an opportunity to encourage broader adoption. But such endorsement is usually predicated upon demonstration of results. Initial adoption and prototyping by stakeholder organizations can prove technical solutions, providing the necessary proof for senior leadership while simultaneously encouraging broader adoption directly. The underlying challenge is to identify organizations with the time, funding, and interest to perform this prototyping.

A conceptual model is used to communicate information about the system represented (including key actions and interactions), limiting assumptions, and simulation capabilities; it's the key connection between the user and the developer. The lack of conceptual modeling standards (SISO SCM) makes development of broadly acceptable cyber conceptual models challenging. But this could also be an opportunity for cyber to provide valuable lessons learned to the broader conceptual modeling problem while improving communication about cyber simulation to potential users.

While many venues exist to conduct cyber for cyber activities, very few venues exist to conduct integrated cyber-kinetic operations testing, training, and experimentation. U.S. Forces Korea's Ulchi Freedom Guardian was one such venue but has been disestablished (Wells, 2015). Operation Blended Warrior (OBW) was another venue that has also been disestablished (Moore, 2018). Additional venues are needed to mature and transition cyber M&S capabilities that are interoperable and sustainable.

The challenge of the classification of cyber data cannot be overstated. Because it is a security challenge, not a technical one, partial solutions are unacceptable. The issue of collecting, safeguarding, and sharing this data prudently must be addressed early and thoroughly.

Finally, funding and support for continuing maintenance and evolution of standards is critical to maintaining technology relevance. While it preserves the value of initial investment, it is much harder to justify than a new technology that is perceived as critical.

CONCLUSION

The purpose of this paper is to propose a roadmap for cyber M&S interoperability. The roadmap includes a vision, description of required capabilities, and recommendations for implementation. The intent is for the DoD, industry, and academia to work in concert to leverage, improve upon, and execute the roadmap across the spectrum of related cyber M&S activities. Without a roadmap, the community at large will most likely develop independent and disparate solutions that will require time and effort to rework in the future. The adoption of a roadmap and associated standards and reference implementations has the potential to significantly improve the timeline and efficiency of cyber M&S interoperability and ultimately, force training and readiness.

ACKNOWLEDGEMENTS

Dr. Morse's contribution to this effort and paper were funded by the Test Resource Management Center.

REFERENCES

Couretas, Jerry M. (2019). *An Introduction to Cyber Modeling and Simulation*, Wiley and Sons.

Guttman, R. (2017). Combined Arms Cyber-Kinetic Operator Training. SEI Blog, Mar 2017.

Headquarters, Department of the Army, Field Manual 3-90-1 (FM 3-90-1) (2013): Offense and Defense Volume1.

Herman, S., Lambert, S., Ostwald, T., & Shostack, A. (2006). Threat Modeling: Uncover Security Design Flaws Using the STRIDE Approach. *Microsoft Developer Network Magazine*, Nov 2006.

IEEE (2012). *Distributed Interactive Simulation --Application Protocols*, IEEE 1278.1-2012, https://standards.ieee.org/standard/1278_1-2012.html

Moore, S.R.; Chaney, M.; & Flint, L. (2018). Cyber Training Experimentation through Operation Blended Warrior. Interservice/Industry Training, Simulation & Education Conference, Dec 2018.

Morse, K.L.; Drake, D.L.; Wells, W.D.; & Bryan, D.S. (2014). Realizing the Cyber Operational Architecture Training System (COATS) Through Standards. Simulation Interoperability Workshop, Sep 2014.

Raymond, David et al, Key Terrain in Cyberspace: Seeking the High Ground. 2014 6th International Conference on Cyber Conflict, NATO CCD COE Publications

SISO RPR, (2015). *Real Time Platform Reference Federation Object Model*, SISO-STD-001-2015, https://www.sisostds.org/DigitalLibrary.aspx?Command=Core_Download&EntryId=30822

SISO SCM, (2006). *Simulation Conceptual Modeling (SCM) SG Final Report*, SISO-REF-017-2006, https://www.sisostds.org/DigitalLibrary.aspx?Command=Core_Download&EntryId=30800

SISO TOR, (2018). *Terms of Reference for the Cyber Modeling and Simulation Study Group*, SISO-TOR-026-2018. https://www.sisostds.org/DigitalLibrary.aspx?Command=Core_Download&EntryId=46159

Wells, W.D. and Bryan, D.S. (2015). Cyber Operational Architecture Training System – Cyber for All. Interservice/Industry Training, Simulation & Education Conference, Dec 2015.