A Cyberspace and Electromagnetic Activities (CEMA) Framework for M&S

Mr. Nathan Vey
U.S. Army Combat Capabilities Development Command - Soldier Center (CCDC-SC)
Orlando, FL
nathan.l.vey.civ@mail.mil

Mr. Timothy Friest, Mr. Jim Ruth
Trideum Corporation
Leavenworth, KS
tfriest@trideum.com, jruth@trideum.com

Mr. Clark Heidelbaugh
Trideum Corporation
Alexandria, VA
cheidelbaugh@trideum.com

LTC Chad Bates, Ph.D.
USA Cyber G37
Ft Belvoir, VA
chad.t.bates.mil@mail.mil

Dr. Mark Riecken
Trideum Corporation
Orlando, FL
mriecken@trideum.com

ABSTRACT

The computer and internet revolutions of the twentieth century have quickly yielded the amorphous concept of "cyber" in the twenty-first century across every enterprise involving computers and networks. The United States Army (USA) modeling and simulation (M&S) enterprise is no exception. The USA has also recognized the connection between cyberspace and electromagnetic activities and has therefore introduced the concept of Cyberspace and Electromagnetic Activities (CEMA). Acknowledging both the challenges of this emerging warfighting domain and the opportunity to provide a systematic framework, the Army Modeling and Simulation Office (AMSO) in cooperation with DEVCOM STTC has undertaken an effort to develop a CEMA M&S Framework (CMFW). The CMFW consists of an ontology based on Army doctrine and informed by all six Army M&S communities of interest (COI). In addition, the CMFW includes use cases and other engineering models that can be used by multiple stakeholders for purposes ranging from developing common models, supporting the development of consistent data exchange models (DEM), and informing program requirements. The methodology used to develop the ontology is a form of Domain Engineering that considers multiple exemplars from across the COI spectrum. This paper discusses both the methodology used to develop the CMFW and provides detail on data, results and other important aspects of the CMFW including the Unified Modeling Language (UML) representation of the ontology. Although this work is sponsored by and performed for the USA, it is takes into account the necessity of multi-domain operations (MDO) and the need to include the perspective of all Services and coalition partners. Lessons learned and challenges are also discussed. As this work continues to mature, the benefit to the Services includes increased commonality in CEMA M&S representation, reduced interoperability issues, and greater efficiencies in training, analysis, test and evaluation (T&E) related to the CEMA domain.

ABOUT THE AUTHORS

Mr. Nathan Vey is a Science & Technology Manager at the U.S. Army Combat Capabilities Development Command - Soldier Center (CCDC-SC), SFC Paul Ray Smith Simulation & Training Technology Center (STTC).

Mr. Clark Heidelbaugh works with Cyberspace and Electronic Warfare Modeling & Simulation for Trideum Corporation. He has over 30 years of organizational leadership experience as a Special Forces officer with CWMD and Counter-IED positions. His operations research studies have informed DoD and U.S. Army strategic decisions, requirements analysis, prioritization and operations. He holds a MS in Systems Engineering, MS in Operations Research, Master's of Strategic Studies-Advanced Strategic Art Program, and Graduate Certificates in C4ISR and Military Operations Research.

LTC Chad Bates, Ph.D. holds a PhD from George Mason University specializing in unmanned aerial systems and remote sensing. LTC Bates is an Army Modeling and Simulation officer (Functional Area 57) currently serving with the U.S. Army's Cyber Command (ARCYBER) as the Chief of Modeling & Simulation as the Deputy G37. LTC Bates has served with the U.S. Army Deputy Chief of Staff for Intelligence (G-2) at the Pentagon where he worked M&S issues for the military intelligence community and also on aerial platforms and their sensor payloads. He earned a bachelor's degree in Human Factors Engineering from the United States Military Academy, and double master degrees from Webster University in Information Systems Management and Human Resources Management. While at the Naval War College in Newport, R.I. he earned another master's degree in National Security and Strategic Studies. He has served combat tours in Iraq and Afghanistan.

Mr. Jim Ruth is a Senior Military Analyst at Trideum Corporation and the Lead Simulation to Mission Command Interoperability (SIMCI) Architect working with Cyberspace and Electronic Warfare Modeling & Simulation. Mr. Ruth has over 20 years of operational assignments in the US Army. His post-military experience includes cybersecurity, architectures, and requirements management. He holds a MS in Computer Resources and Information Management and professional certificates for Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP), and Information Assurance (IA)/ Chief Information Officer (CIO).

Mr. Tim Friest is a software developer for Trideum Corp. has worked as a defense contractor for over 25 years, developing interoperability standards and solutions for mission command and modeling and simulation.

Dr. Mark Riecken is Chief Engineer at the Trideum Corporation. He has over 30 years of experience in modeling & simulation, systems engineering, and command and control. He has a Ph.D. in Electrical Engineering from the University of New Mexico.

A Cyberspace and Electromagnetic Activities (CEMA) Framework for M&S

Mr. Nathan Vey
U.S. Army Combat Capabilities Development Command - Soldier Center (CCDC-SC)
Orlando, FL
nathan.l.vey.civ@mail.mil

Mr. Timothy Friest, Mr. Jim Ruth
Trideum Corporation
Leavenworth, KS
tfriest@trideum.com, jruth@trideum.com

Mr. Clark Heidelbaugh
Trideum Corporation
Alexandria, VA
cheidelbaugh@trideum.com

LTC Chad Bates, Ph.D.
USA Cyber G37
Ft Belvoir, VA
chad.t.bates.mil@mail.mil

Dr. Mark Riecken
Trideum Corporation
Orlando, FL
mriecken@trideum.com

INTRODUCTION

The U.S Department of Defense (DoD) continues to openly and formally acknowledge the challenges of cyberspace facing the Nation with the publication of the 2018 DoD Cyber Strategy (Department of Defense, 2018). This strategy recognizes the need to prepare for cyber operations as an integral part of modern warfare as well as the necessity to work with other partners to counter daily cyber threats to the Nation. Knowing the importance and significance of the challenges posed by these goals during the few years leading up to this publication, the Army's Modeling and Simulation (M&S) community began to develop cyber-related tools, models and services to be able to represent cyberspace operations during peacetime and wartime. In an effort to "build once and reuse often," the Army's M&S community organized the Cyber Electronic Warfare (EW) M&S Working Group (CyEWMS WG) to identify M&S gaps and guide Army M&S investments. In 2016, this group identified the lack of a "framework" that could guide developmental efforts, synchronize investments and seek to increase return on investment was a significant gap. Particularly the group desired this project to deliver a Cyberspace and Electromagnetic Activities (CEMA) Framework that would relate M&S to:

- Newness and unfamiliarity of the Cyberspace domain;
- Development of CEMA terminology and concepts in the "real world:"
- Different perspectives and needs of the various M&S communities of interest (COI) and their projects;
- The magnitude of the CEMA problem space in the "real world."

This paper highlights many facets of a project intended to close this gap. We address the progress of the CEMA framework project for developing M&S tools, models and services, which will assist the Army to train and equip its forces to conduct cyberspace operations as part a joint military force that spans peacetime and wartime operations.

THE PROBLEM AND THE OPPORTUNITIES

The term "CEMA" was first used less than a decade ago (Delacruz, n.d.). This relatively new term encompasses concepts that are not especially new: cyberspace operations, electronic warfare (EW), and spectrum management operations (SMO). The term does, however, justifiably highlight the newness of an important problem space. It underscores the explosive magnitude of cyberspace and the growing interconnectedness of kinetic and non-kinetic effects. It also emphasizes the integration of traditional disciplines such as EW with the newer concepts of cyberspace operations. In this paper, CEMA is a U.S. Army term, not necessarily shared by other Services or coalition partners, reflecting the unique mission and perspective of the Army. All these factors contribute to the problem of finding common ground among the many stakeholders. This common ground is needed to provide an adequate foundation from which to develop the required and enduring modeling and simulation (M&S) capabilities for the warfighter and decision makers.

This challenge also represents an opportunity. The kinetic M&S world evolved over several generations in a largely asynchronous manner driving the need for interoperability tools and capabilities. The real world demands of CEMA, especially the cyberspace operations component, are propelling a sense of urgency to provide M&S solutions across all COI. Can the M&S community act rapidly and in a coordinated manner to achieve a more standard approach to non-kinetic (i.e., CEMA) M&S? If this is at all possible, a modeling framework that supports a reasonably comprehensive common vocabulary, and, to some degree, common software and data elements, is needed. Of course, perfect coordination across the diverse M&S community is not possible and it is clear that many robust CEMA M&S efforts are well underway. The challenge and opportunity for this effort then narrows to the problem of identifying gaps in needed M&S representations and searching for potential commonality of approaches.

The Role of CEMA in 21st Century Conflict

During periods of conflict, the Army will fight in a joint, multi-service, context. The joint operational doctrine for Cyberspace Operations, Joint Publication 3-12, considers the domain of cyberspace to contain three layers, the physical, the logical and the cyber-persona (Joint Staff, 2018). Each layer, with its own complexities, comprises the human-constructed domain that resides within the other physical domains, land, maritime, air and space. To describe military operations across these domains, the Army recognizes the relationship and connections in its publication on Multi-Domain Operations, which includes wartime operations in multi-domain battle (United States Army, 2018). The image in **Figure 1** illustrates CEMA across the domains as represented from Army Field Manual (FM) 3-12 Cyberspace and Electronic Warfare Operations (HQ DA, 2017). Each node and connection represents the connections of the physical, logical and cyber-persona layers.

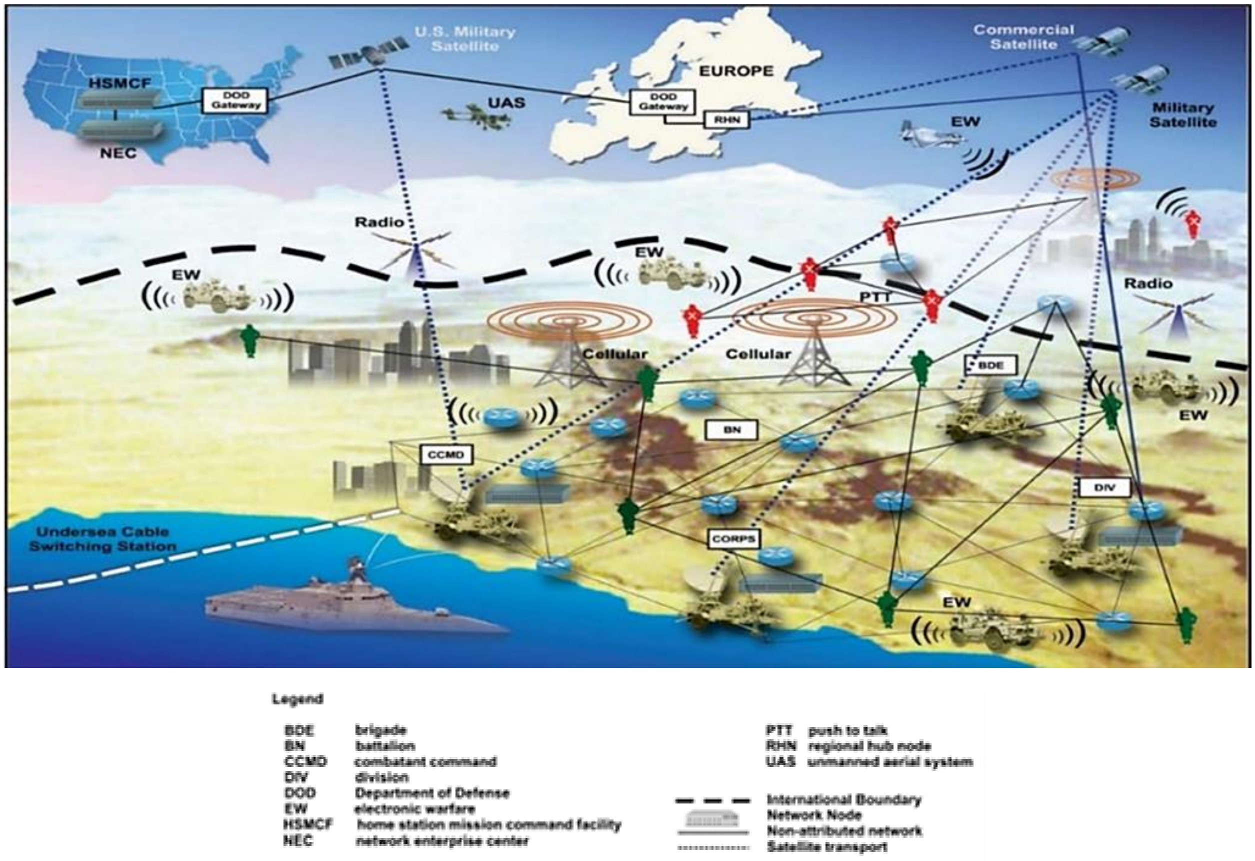

Figure 1 A Visualization of Cyberspace, An Operational Context ("CEMA OV-1") *(HQ DA, 2017)*

Key aspects can also be grouped as depicted in the CEMA Operational Framework in **Figure 2** from FM 3-12. The domains, physical architectures, constructs, activities and entities depicted in this figure challenge Army users, developers, and analysts to create accurate representation in models and simulations. These tools, as with other M&S developments, will enable understanding of cyberspace-related effects. The current thinking of Army M&S practitioners reflects a grouping of M&S efforts that focus on three categories of audiences: Cyber for Cyber, Cyber for Others and Cyber for All.

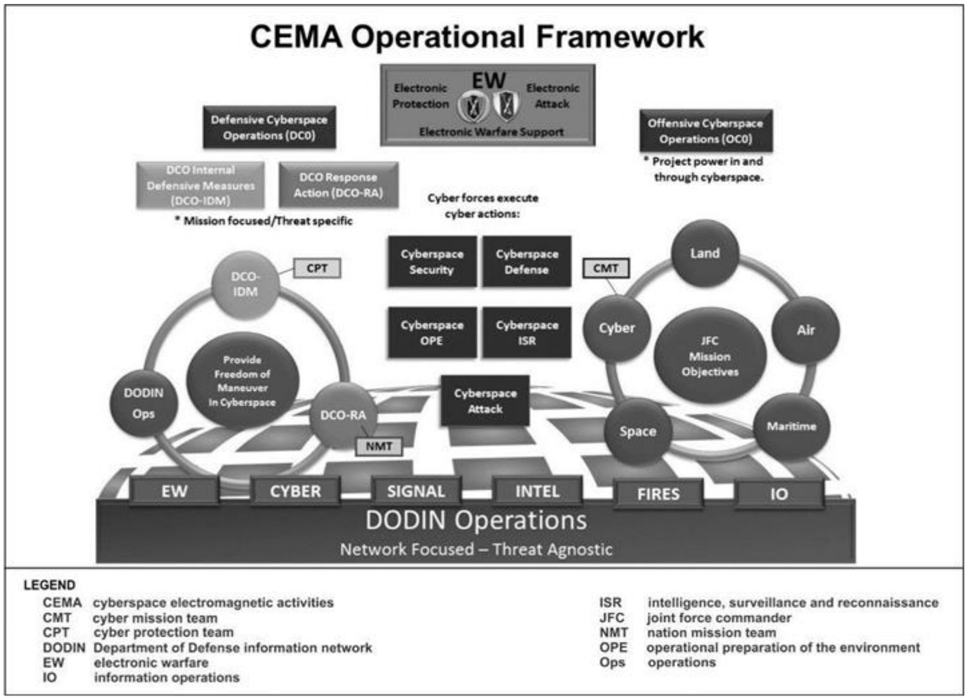
CEMA Operational Framework
EW
Electronic Protection
Electronic Attack
Electronic Warfare Support
Defensive Cyberspace Operations (DC0)
DCO Internal Defensive Measures (DCO-IDM)
DCO Response Action (DCO-RA)
* Mission focused/Threat specific
Offensive Cyberspace Operations (OC0)
* Project power in and through cyberspace.
Cyber forces execute cyber actions:
Cyberspace Security
Cyberspace Defense
Cyberspace OPE
Cyberspace ISR
Cyberspace Attack
CPT
DCO-IDM
Provide Freedom of Maneuver In Cyberspace
DODIN Ops
DCO-RA
NMT
CMT
Land
Cyber
JFC Mission Objectives
Air
Space
Maritime
EW
CYBER
SIGNAL
INTEL
FIRES
IO
DODIN Operations
Network Focused – Threat Agnostic
LEGEND
CEMA cyberspace electromagnetic activities
CMT cyber mission team
CPT cyber protection team
DODIN Department of Defense information network
EW electronic warfare
IO information operations
ISR intelligence, surveillance and reconnaissance
JFC joint force commander
NMT nation mission team
OPE operational preparation of the environment
Ops operations

Figure 2 CEMA Operational Framework from Doctrine (FM 3-12) (HQ DA, 2017)

Each of the cyberspace M&S audience categories contain focus areas and areas for application.

- Cyber for Cyber (M&S Characteristics: High fidelity, full pathway)
    - Replicate conditions for training, testing, analysis and experimentation (Individual/Collective; Validation Exercises; Mission Rehearsals)
    - Bridging solutions for Persistent Cyber Training Environment (PCTE)
- Cyber for Others (M&S Characteristics: Low/High Fidelity – Effects on Systems)
    - Replicate CEMA conditions for training, experimentation, analysis, testing
    - Effects on individual equipment
    - Impacts on communications, radars, operations centers
    - Identify gaps in M&S, assist in problem definition
    - Create a common lexicon, tactical and technical
    - Training Centers
- Cyber for All (combines Cyber for Cyber and Cyber for Others)

To address these M&S focus areas, the Army's M&S communities intend to incorporate the outcomes of the CEMA M&S Framework project to enable re-use through common ontology and understanding.

Why is CEMA M&S Important?

Although communications effects (something less than perfect communications) have been modeled and simulated for some time (e.g., (Cloutier, Korfiatis, & Thompson-Bass, 2012)), as well as electromagnetic propagation and EW effects (e.g., (Adamy, 2006)), we assert that the preponderance of military M&S has remained focused on kinetic effects, rather than non-kinetic. This tracks the path of distributed computing itself, over the past several decades, which has been remarkable in achieving the current level of sophistication in simulated kinetic battlespace interactions. However, since CEMA has the potential to have an effect on everything in the battlespace, neglecting these CEMA effects in M&S is to do injustice to the problem of battlespace representation in M&S.

APPROACH

Our approach to this problem was to construct a conceptual model of CEMA as it is found in the operational world (based on doctrine) and to also develop a separate model based on existing or emerging M&S representations of CEMA. The comparison of these two models should provide insight into both gaps and opportunities for commonality. The results of this model comparison not only allow initial findings but provides the basis for an ongoing and systematic process.

What is a CEMA M&S Framework?

There are many different and pre-conceived notions for the concept of a framework. Our framework must meet the following requirements: 1) It should use standard engineering tools and techniques; 2) it should enable communications with a common vocabulary; 3) it should be implementable at least at the interface level; and 4) it should provide a systematic means of identifying potential commonality in M&S as well as gaps.

From a practical viewpoint, there are four major components to the CEMA M&S Framework (CMFW).

- Ontologies and models. The ontologies and models expressed in Unified Modeling Language (UML) provide a standards-based means for describing common vocabulary and relationships between terms and concepts. We use Sparx Systems Enterprise Architect (EA) tool, but any similar tool would serve the same purpose.
- M&S Architecture & Code Elements. We use UML to identify and describe M&S software architecture elements, including data exchange models (DEM). The DEM currently in the CMFW reflects a snapshot of the Simulation Interoperability Standards Organization (SISO) Cyber M&S Study Group work.
- Gaps and Issues Spreadsheet. A fundamental purpose of the CMFW is to help identify gaps. Therefore, an integral part of the CMFW is a means of tracking gaps and issues. We currently use a spreadsheet.
- Governance Plan. Since the CMFW is intended for extended use, it requires an owner, a means of managing the maintenance, and a reasonable process of adjudicating decisions.

Hybrid Approach: Sparse Domain Analysis, the Kinetic M&S Analogy and First Principles

Our approach borrows heavily from the discipline of Domain Engineering (Kang, Cohen, Hess, Novak, & Peterson, 1990). As part of establishing a systematic approach to identifying gaps in CEMA M&S, we developed two[1] domain models as shown in **Figure *3***. Since this effort is motivated primarily by the need to efficiently discover "gaps" in current CEMA M&S, as well as opportunities for commonality, a Domain Engineering approach in which a baseline model can be compared with current exemplars provides a systematic means to achieve this goal.

[1] More accurately stated, we developed two *sets* of domain models; for the sake of clarity, we consider these two UML *model sets* as singular UML models.

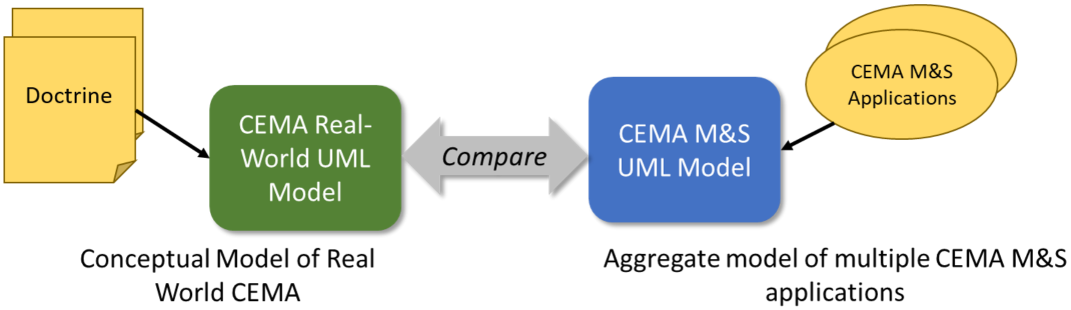
Doctrine
CEMA Real-World UML Model
Compare
CEMA M&S UML Model
CEMA M&S Applications
Conceptual Model of Real World CEMA
Aggregate model of multiple CEMA M&S applications

Figure 3 Searching for Gaps (and Commonality) in CEMA M&S

The first model is a representation of the real-world "domain"[2] of CEMA defined largely by doctrine, e.g., (HQ DA, 2017); this is a model of CEMA from a doctrinal perspective and does not necessarily reflect what features should be represented in M&S nor what simulation-specific considerations might be needed. The second model (really an amalgam of multiple models) is comprised of current and emerging CEMA M&S exemplars such as the data model from the CyberBOSS (Vey, 2019) project. The so-called real-world model then provides a basis for what *might* be needed in a CEMA M&S model. It is certainly not all inclusive, but it has proven to be a useful checklist against which to compare the current CEMA M&S implementations.

RESULTS

The approach described above is limited by available data, especially on the CEMA M&S model side. It takes time for all parties to go through a process of requesting releasable data that can be freely incorporated into this approach. There are potential releasability issues both from a Controlled Unclassified Information (CUI) perspective as well as from a proprietary data perspective. On the doctrine side, we note that the doctrine is new and arguably still evolving. Nonetheless, this approach is useful in developing a tangible product that can be employed in a systematic process. In addition, in order to provide comprehensive Army coverage, we have attempted to engage with all six of the Army M&S communities of interest (COI)[3] per AR 5-11 (Army Modeling and Simulation Office, 2014). To date, we have engaged representatives from Training, Test and Evaluation, and Analysis. Some of the most visible and successful efforts have been in the Training community (Wells & Bryan, 2018).

The CEMA M&S Framework

The CEMA M&S Framework as shown in **Figure *4*** is composed of a set of UML models that define ontologies and architectural components that represent CEMA in simulations across the AMSO M&S COIs (e.g. it is applicable to more than just a single COI like training or test & evaluation).

[2] We recognize that CEMA is not considered a "domain" on a par with Air, Land, Sea, and Space. The term *domain* is used here in the sense of domain engineering and analysis.

[3] The six communities are Acquisition, Analysis, Experimentation, Intelligence, Test and Evaluation, and Training.

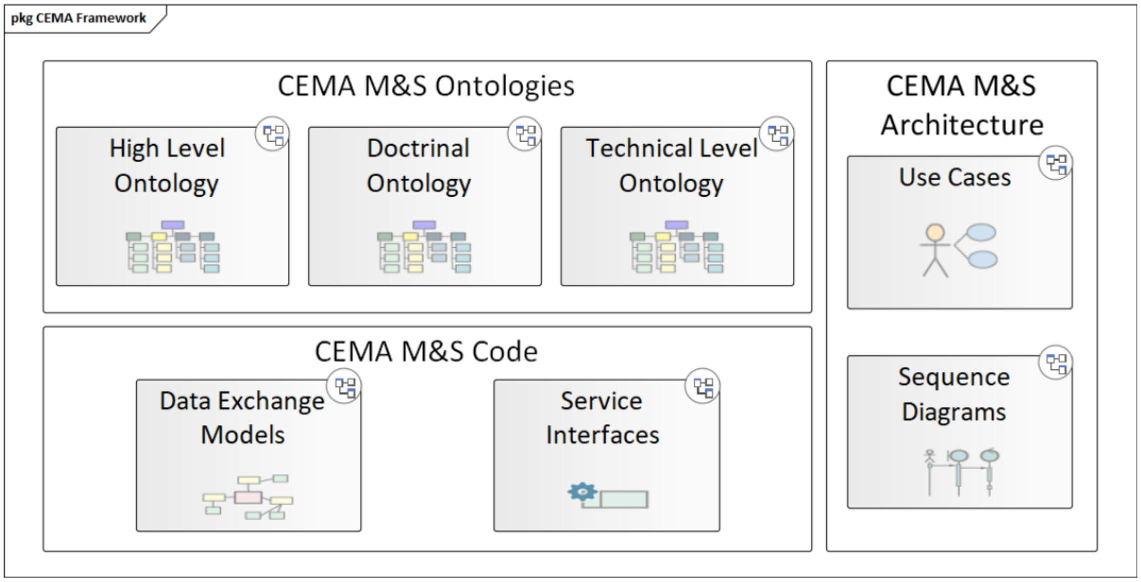

Figure 4 CEMA M&S Framework

The CEMA M&S Framework Ontologies. An ontology defines a set of concepts in a domain (of knowledge), their properties and the relationships between them. The Framework defines three models to capture different levels of CEMA concepts:

- a high-level model that frames CEMA in the context of military M&S
- a doctrinal/operational level model that describes CEMA concepts for operational commanders/units
- a technical level model which defines the low-level concepts of CEMA actions/effects

The high-level ontology (**Figure** *5*) defines the over-arching concepts of CEMA M&S and frames them with respect to other (non-CEMA) concepts for M&S of military operations. It describes concepts (classes in the diagram) that fall into several broad groupings (shown below with blue circles). The four physical domains are represented in addition to the cyberspace domain, where cyberspace resides within the information environment. Cyberspace is made up of three layers, and network topologies are also represented as cyber terrain. CEMA are a kind of activities; specific actions result in effects that impact kinetic (physical), CEMA (cyberspace and/or electromagnetic), or human behaviors.

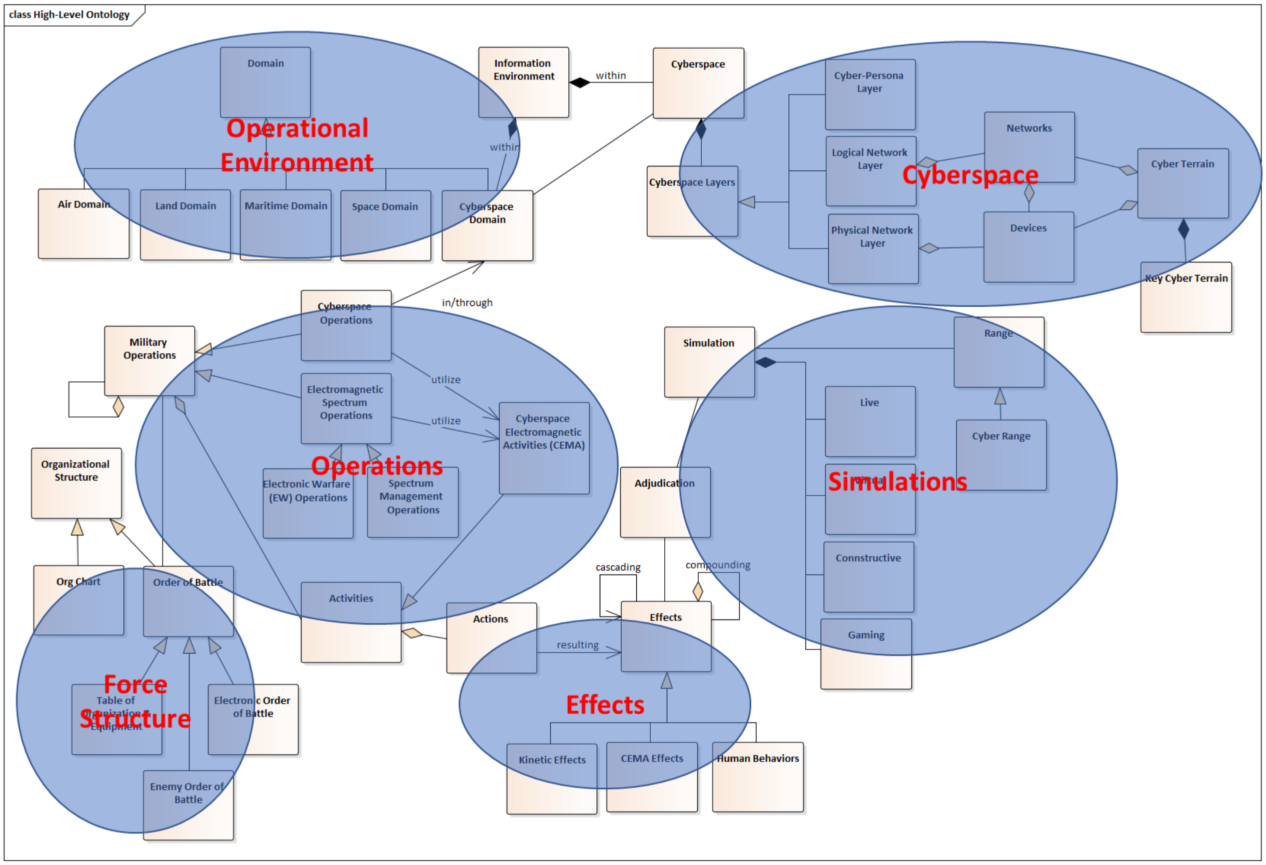

Figure 5 High-Level Ontology

A doctrinally based Ontology (**Figure *6***) reflects the CEMA concepts of interest to commanders and staff of operational units. It is heavily based on Army (FM 3-12) and Joint (JP 3-12 and JP 3-13.1) doctrine for cyberspace, EW, and signal management operations. Threats and tactical level effects are also represented. Significant concepts include the differentiation of actions for attack, security/defense/protection, and Intelligence, Surveillance and Reconnaissance / Operational Presentation of the Environment (ISR/OPE) support.

Note that Cyberspace and Electronic Warfare operations utilize actions, which are further classified as attack, defense/security/protection, or supporting (support for EW or ISR/OPE for cyberspace). Attack actions result in effects that are described using traditional fires effects terms.

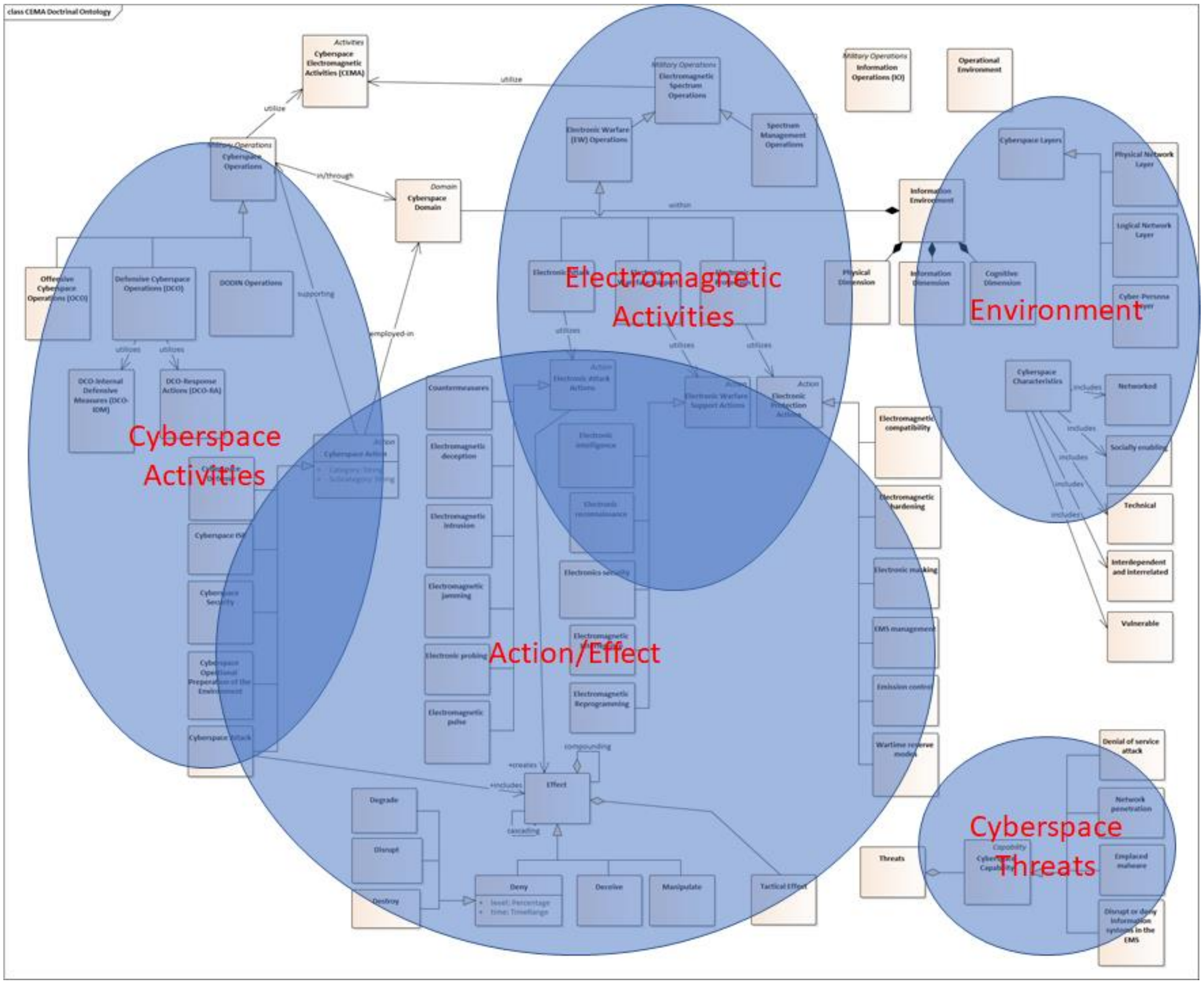

Figure 6 Doctrinal Ontology

Finally, a Technical Level Ontology (**Figure *7***) defines the technical details of CEMA, that need to be supported in simulations, to represent specific effects on physical devices/systems. Cyberspace actions directly affect the software on devices or the information that resides or flows through the devices. It is therefore necessary to model devices and networks (cyber terrain) as well as the relevant actions and effects. This level of modelling also allows the simulations to handle cross domain effects (e.g. a kinetic effect destroying a network node has cascading cyberspace effects of denying messaging traffic).

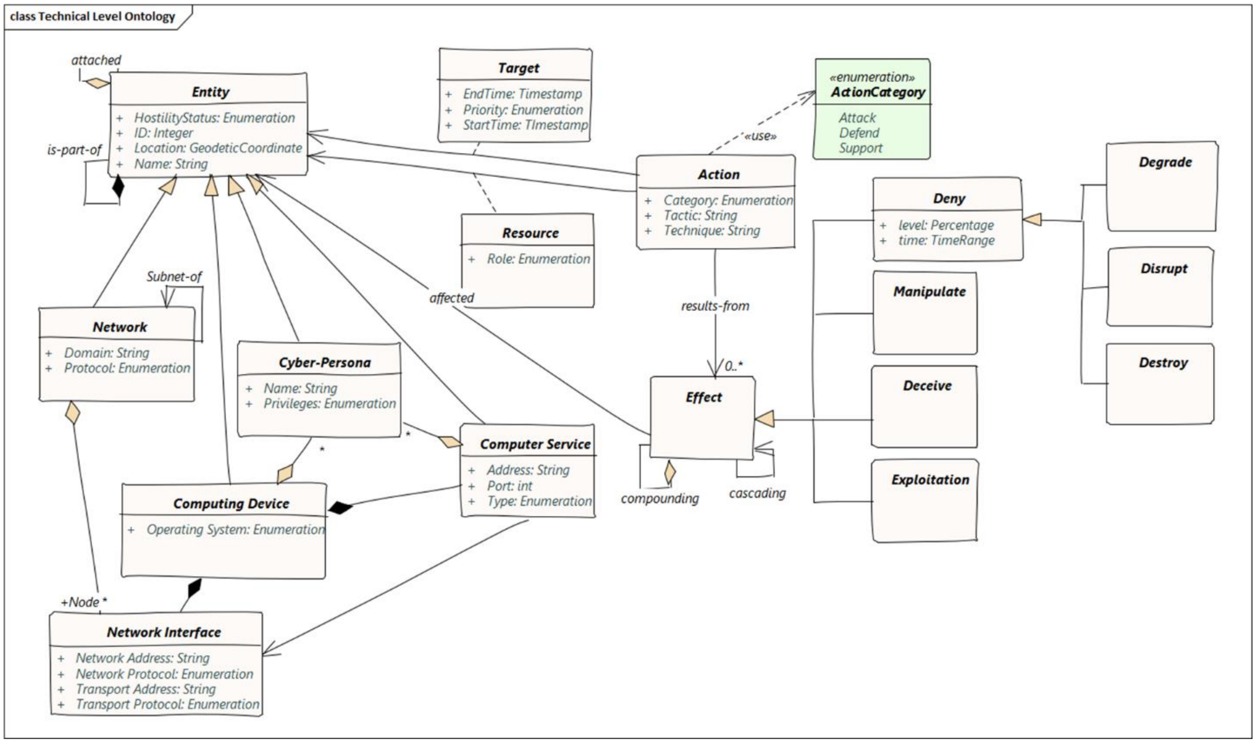

Figure 7 Technical Level Ontology

CEMA M&S Framework Architecture and Code. The framework also identifies architectural components, such as services and data exchange models, that should typically be present in a simulation (that supports CEMA). **Figure *8*** is a model that depicts a recent draft version of SISO Cyber M&S Study Group data exchange model (DEM).

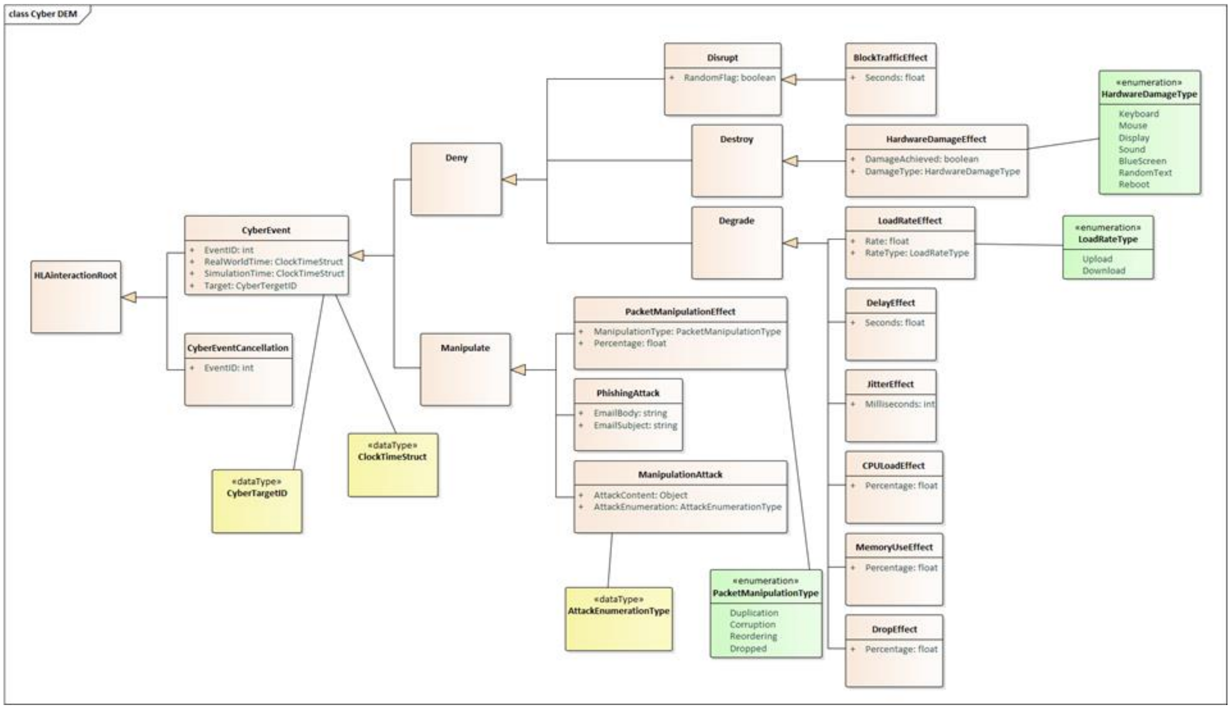

Figure 8 Draft Cyber DEM

Emerging Gaps, Commonalities, and Issues Across the COI

The CyEWMS WG has identified and continues to identify CEMA M&S gaps, which is the term for a lack of M&S representation of desired or actual operational capability. The CMFW includes those gaps using a Gaps and Issues spreadsheet. **Table *1*** highlights selected gaps and issues.

Table 1 Highlighted Gaps and Issues in CEMA M&S

Topic Area	Description	Gap or Issue
CEMA and PNT	Several of the gaps highlight the relationship between CEMA and Position, Navigation, and Timing (PNT), as well as Assured PNT (APNT)	Gap
Kinetic and non-kinetic Integration	Although there is important work in this area, especially the Cyber Kinetic Effects Integration (CKEI) at Carnegie Mellon University (CMU) (Guttman), there remain significant challenges to delivering this capability to the wide variety of models and simulations in the inventory.	Gap
CEMA and Network Representations	The relationship between the many network M&S efforts and CEMA M&S have yet to be fully explored.	Gap
Information Representation and relationship of CEMA to Information Operations (IO)	Information is at the heart of CEMA-related concepts whether that information is being protected, destroyed, or exploited. Furthermore, a physical device may be compromised without compromising information. Therefore, in some cases, the explicit modeling of information may be required.	Gap
CEMA M&S Aggregation/ De-aggregation	CEMA effects may be modeled at various levels of resolution (e.g., by IP address, OSI stack, aggregations of networks/cloud) by different models or within the same model.	Issue
Cascading effects of CEMA	FM 3-12 mentions that effects can be cascading or be accomplished by an accumulation of other effects.	Issue

How to Use the CEMA M&S Framework – An Important Use Case

The CyEWMS WG has participants from across the Army and other services. The participants represent groups of M&S users that include several major functional groups, including: Military Operators and Planners, M&S requirements and capability managers, and M&S Developers. The CMFW provides these groups with a common approach to communicate about cyberspace and electromagnetic activities. The purpose of the CyEWMS WG is to discover M&S gaps (as well as to identify duplicative or common efforts). Once the gaps (or commonality) are identified, seedling project are identified that may be funded. The challenge facing the WG has been where to start and what method to use for a judiciously systematic coverage of such a large space. **Figure *9*** illustrates the workflow for this use case. Starting from the top left quadrant, the ontologies are built (and maintained). As discussed earlier (see **Figure *3***), there are two sets of ontologies: one built from doctrine and the other from "as-built" M&S. The comparison of these two data sets in a systematic way greatly facilitates gap discovery. In the top right and bottom right quadrants, the WG "traverses" the ontologies to discover potential gaps. We note that just because no M&S exists for a given doctrine-based feature, it does not mean that it is a gap that must be filled. Finally, the WG uses the identification of gaps (or commonality) to develop project descriptions, seek sponsors and funding to address the need as appropriate. This important use case has its own Governance Plan that identifies major stakeholders with roles, responsibilities, and authority (RRA) and other elements to support the maintenance of this effort.

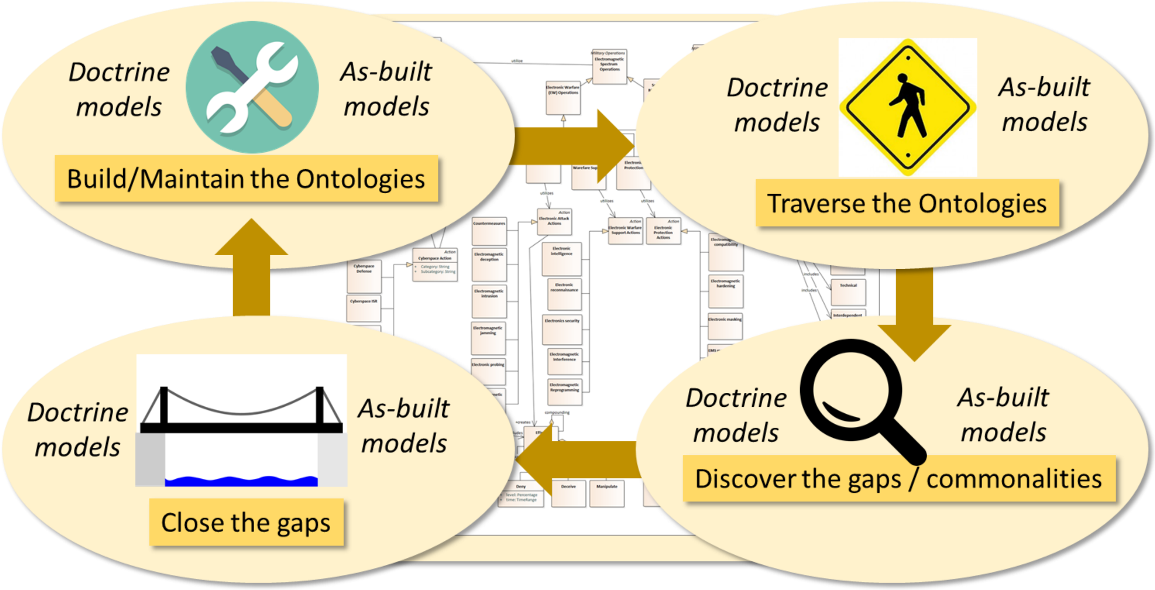

Figure 9 The CyEWMSWG CMFW Use Case - Finding Gaps

The CEMA M&S Framework's Future – Evolving Toward Information Warfare?

In support of DoD Cyber Strategy, the US Army has adopted of a cyberspace domain as one of the five domains in Multi-Domain Operations (MDO) (United States Army, 2018). This indicates that CEMA continues to be a component of military operations for the foreseeable future. The adoption of cloud technologies in government and civilian organizations across the globe indicate the pervasiveness of CEMA-like behaviors.

> *The 2018 Department of Defense Cyber Strategy states: "The Department must take action in cyberspace during day-to -day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests."*

At the tactical level, the Modified Combined Obstacle Overlay (MCOO) underpins the commander's considerations for maneuver warfare tasks, the Combined Information Overlay (CIO) (Rittenberg, Barry, Hickey, Rhee, & Cross, 2019) will provide the basis of the commander's information warfare tasks. CEMA concepts provide the functional description of where information warfare is executed in cyber, electronic warfare (EW), and frequency spectrum components.

Current concepts on Cyber-for-Cyber and Cyber-for-Others continue to coalesce into Cyber-for-All as Information Warfare concepts mature. Future Soldiers and leaders become aware of the constant bombardment of information operations attempting to influence their decisions and takes appropriate steps to nullify those effects.

Lt. Gen. Stephen Fogarty, USA, commanding general, Army Cyber Command (ARCYBER), is transforming ARCYBER into the Information Warfare Command over the next 10 years (Underwood, 2019). CEMA is contained in current doctrine and will undergo a simultaneous transformation to become inclusive of the activities to support information operations and warfare.

CEMA M&S becomes more critical for the accurate replication of the future information environments where military forces will operate. As part of the overall M&S Enterprise, this CEMA M&S Framework should evolve and mature or possibly be replaced with an Information Operations/Warfare M&S Framework that will capture the evolving nature of the cyberspace domain and how to best represent it. Information Operations/Warfare M&S assists in the acquisition of the correct capabilities and material and supports the suitable training to prepare Warfighters to win the next conflict.

SUMMARY AND CONCLUSIONS

We have presented a description of a CEMA M&S Framework. The purpose of this framework is to facilitate communication within the CEMA M&S and broader M&S and military communities with a need to understand the implications of CEMA on military operations. The CMFW consists of a UML-based ontology, software architecture elements, and a spreadsheet of gaps and issues. A CMFW Governance Plan was also developed to provide a lightweight means of managing the CMFW.

CEMA M&S continues to prove to be a challenging topic area not the least because it essentially overlays and influences all of the kinetic world as well as the information sphere. We have found that the M&S Training community has moved out aggressively in developing CEMA M&S. We have also found that there remains an overall strategic opportunity to develop CEMA M&S in a systematic fashion. Even if this cannot be perfectly achieved, we believe the CMFW approach can yield significant return in development and execution efficiencies.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the invaluable help from the following individuals and organizations in this project: Dr. Ken LeSeuer, Redstone Test Center, and the Cybersecurity Vulnerability Assessment Test Environment (CVATE) team; Mr. David Silvernail, SMDC; Mr. Skip Tornquist, TSMO; Dr. Fuzzy Wells, IST; Dr. Katherine Morse, JHU, Mr. Gary Waag, SAIC, and the SISO Cyber M&S Study Group; COL Joe Nolan, AMSO, and the Cyber/Electronic Warfare M&S Working Group; Dr. Nancy Bucher; Dr. Bill Hopkinson and the DoD Cyber Modeling and Simulation Technical Working Group. We also thank Dr. Joe McDonnell for a close reading of our final draft.

REFERENCES

Adamy, D. L. (2006). *Introduction to Electronic Warfare Modeling and Simulation.* Scitech Publishing.

Army Modeling and Simulation Office. (2014). *Management of Army Modeling and Simulation.*

Cloutier, R., Korfiatis, P., & Thompson-Bass, K. (2012). *Communications Effects Server (CES) Model for Systems Engineering Research.* Stevens Institute of Technology, Systems Engineering Research Center. Retrieved from https://web.sercuarc.org/documents/technical_reports/1530637722-SERC-2012-TR%20025-1%20Communications%20Effects%20Server%20RT%20023.pdf

Delacruz, V. (n.d.). *Mission Command In and Through Cyberspace: A Primer for Army Commanders*. (U.S. Army) Retrieved April 30, 2019, from The Cyber Defense Review: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136047/mission-command-in-and-through-cyberspace-a-primer-for-army-commanders/

Department of Defense. (2018). *DOD Cyber Strategy.* Retrieved May 10, 2019, from https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Guttman, R. (n.d.). *Combined Armys Cyber-Kinetic Operator Training.* Retrieved May 3, 2019, from https://insights.sei.cmu.edu/sei_blog/2017/03/combined-arms-cyber-kinetic-operator-training.html

HQ DA. (2017). FM 3-12 Cyberspace and Electronic Warfare Operations.

Joint Staff. (2018). Joint Publication 3-12. *Cyberspace Operations*.

Kang, K. C., Cohen, S. G., Hess, J. A., Novak, W. E., & Peterson, A. S. (1990). *Feature-Oriented Domain Analysis (FODA) Feasibility Study.* Carnegie Mellon University / Software Engineering Institute.

Rittenberg, L. J., Barry, M. M., Hickey, M., Rhee, M., & Cross, C. (2019). Integrating Information Warfare Lessons Learned from Warfighter Exercise 18-2. *Military Review*, 100-107.

Syed, Z., Padia, A., Finin, T., Mathews, L., & Joshi, A. (2016). UCO: A Unified Cybersecurity Ontology. *The Workshops of the Thirtieth AAAI Conference on Artificial Intelligence. Artificial Intelligence for Cyber Security*, pp. 195-202. AAAI.

Underwood, K. (2019). Army Cyber to Become an Information Warfare Command. *Signal*.

United States Army. (2018). *The U.S. Army in Multi-Domain Operations 2028.*

Vey, N. (2019). Cyber Battlefield Operating System Simulation (CyberBOSS). *2019 Simulation Innovation Workshop (SIW).* Orlando: Simulation Interoperability Standards Organization.

Wells, D., & Bryan, D. (2018). Cyberspace Training - Is This Even Legal? *I/ITSEC 2018.* Orlando.