Using Cyberspace Electromagnetic Activities M&S for Multi-Domain Operations Challenges

COL Chad Bates, Ph.D.
US Army Cyber Command
Fort Belvoir, VA
chad.t.bates.mil@mail.mil

Mr. Clark Heidelbaugh, Mr. Jim Ruth
Mr. Tim Friest, Dr. Mark Riecken
Trideum Corporation
cheidelbaugh@trideum.com, jruth@trideum.com
tfriest@trideum.com, mriecken@trideum.com

ABSTRACT

Given the challenges facing our Nation and allies from the Cyberspace domain, it has become an imperative to provide robust and appropriate representation of Cyberspace Electromagnetic Activities (CEMA) for use in the modeling and simulation (M&S) enterprise. Not surprisingly, achieving that imperative has resulted in the discovery of many gaps in CEMA M&S. There have been a few surprises over the past year that revealed new and unexpected vulnerabilities in the digital fabric of our commercial, industrial, and other sector infrastructures. The CEMA M&S Framework (CMFW) initiative (Vey, et al., 2019) provides a Models Based Systems Engineering (MBSE) approach to systematically survey the breadth of CEMA M&S. The CMFW is primarily focused on the needs of U.S. Army CEMA M&S. In 2021, the CMFW initiative aimed to incorporate Army modernization needs into the framework. To do this, we expanded the framework beyond its original foundation to include Use Cases and Mission-based Operational Threads representing critical process flows that correspond to new approaches being developed for the Army to address Multi-Domain Operations (MDO). The resulting framework can be used as a starting point for CEMA M&S representation for key Army systems to include artillery (Long Range Precision Fires), ground combat vehicles (Next Generation Combat Vehicle), aviation (Future Vertical Lift), as well as other priority areas. Our work provides a common model foundation for future CEMA M&S representation. This foundation does not dictate a single approach to all CEMA M&S problems but does provide a common reference for capability developers and commanders. Our approach strikes a balance between very high level "effects only" modeling and what might be considered a digital engineering (DE) representation to guide capability development for CEMA M&S.

ABOUT THE AUTHORS

COL Chad T. Bates, Ph.D. holds a PhD from George Mason University specializing in Geospatial Information Science. He is an Army Modeling and Simulation officer (Functional Area 57) currently assigned as Special Assistant to the Commanding General, U.S. Army's Cyber Command (ARCYBER). Prior to this assignment, COL Bates served with the U.S. Army Deputy Chief of Staff for Intelligence (DCS G-2) on M&S issues for the military intelligence community. His other academic degrees include a BS in Human Factors Engineering from the United States Military Academy, a double master's degrees from Webster University in Information Systems Management and Human Resources Management, and a master's degree in National Security and Strategic Studies from the Naval War College. He is a combat veteran with tours in Iraq and Afghanistan.

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 (OR) studies informed DoD and U.S. Army strategic decisions. He holds a MS in Systems Engineering, MS in OR, Master's of Strategic Studies-Advanced Strategic Art Program, and Graduate Certificates in C4ISR and Military Operations Research and a BS in Engineering Physics.

Mr. Jim Ruth is a is a Senior Military Analyst at Trideum Corporation and a Simulation to Mission Command Interoperability (SIMCI) Architect working with MC, 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 Corporation. Tim 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 is a long-time contributor to the DoD M&S community. He holds bachelor's and master's degrees in physics and a Ph.D. in Electrical Engineering from the University of New Mexico.

Using Cyberspace Electromagnetic Activities M&S for Multi-Domain Operations Challenges

COL Chad Bates, Ph.D.
US Army Cyber Command
Fort Belvoir, VA
chad.t.bates.mil@mail.mil

Mr. Clark Heidelbaugh, Mr. Jim Ruth
Mr. Tim Friest, Dr. Mark Riecken
Trideum Corporation
cheidelbaugh@trideum.com, jruth@trideum.com
tfriest@trideum.com, mriecken@trideum.com

INTRODUCTION

Which statement is worse: "My COP[1] is not updating," or "Everything looks fine, sir, right on plan." The first is clearly bad, but the second may be just as bad or worse if the COP has, unbeknownst to the observer, been subjected to a non-kinetic attack. It may appear correct but be just incorrect enough to soon cause havoc. Understanding the causes of both situations is mission essential in the highly connected world of MDO.

Throughout military history, introduction of new technology creates new modes of warfare; by contrast, sometimes the science of armed conflict creates technology out of necessity. The relationship between the U.S. Army's Cyberspace Electromagnetic Activities (CEMA) and Multi-Domain Operations (MDO) is one such interdependent and complex pairing in modern warfare. Cyberspace activities, incorporated as part of CEMA, have a dual use aspect as well. The last several decades of exponential growth in computing and network technology have enabled cyberspace weaponization and have blurred the boundaries between competitive commerce and hostile actions, which enable state-backed and non-state actors both more than perhaps ever before. Cyber effects, now joined with Electronic Warfare (EW) and Spectrum Management Operations (SMO) to create a combined discipline of non-kinetic warfare activities referred to as CEMA (Department of the Army, April, 2017) (Army Modeling & Simulation Office, 2021). CEMA has facilitated the inception of MDO in which all battlespace activities have the potential to affect one another with a powerful immediacy. The M&S community can and must use its disciplined processes and technologies to examine and better understand MDO and its role in current and future conflicts.

In these still early days in the development of both CEMA and MDO, we have an opportunity to better codify and structure our approach to CEMA M&S to gain needed insights and contribute to critical national security concerns. In this paper, we list several challenges and opportunities in this problem space. We believe that many of these can be aided by a modeling framework. We then provide a short discussion about MDO and the inherent role of CEMA followed by our results and findings to date through brief examinations of various aspects of the CEMA M&S Framework (CMFW) to include ontologies and mission threads. We note, as a further example of the importance of this area of inquiry, the potential for CEMA and MDO to overlap with Digital Engineering.

CHALLENGES AND OPPORTUNITIES

The use of CEMA M&S to support MDO presents both challenges and opportunities. The challenges are many. 1) The combined discipline of CEMA (Cyber, EW, and SMO) is less than a decade old. The doctrine is new and evolving. Many of the tools and techniques needed to support this discipline are still being developed. 2) CEMA is pervasive in MDO, so it is sometimes difficult to isolate CEMA activities and effects. This means that it can be difficult or impossible to model CEMA in isolation from kinetic activities and effects. 3) There remains a broad lack of understanding throughout the U.S. military and a need to train and educate operational force commanders and their staffs. 4) Like the representation of EW effects for M&S, CEMA M&S can be disruptive to represent (model) and simulate in many events such as a training exercise. This oftentimes mean that training and experimentation events are not exposed to the full spectrum of contingencies that CEMA introduces into operations for fear of stopping progress on other non-CEMA event objectives. 5) Many of the CEMA M&S gaps are well documented through the Cyber EW M&S Working Group (WG) forum at the Army Modeling and Simulation Office (AMSO) (Army Modeling & Simulation Office, 2021). The need for the incorporation of non-kinetic activities and effects in force-on-force simulations is an example of one such gap.

[1] Common Operating Picture

For applications in training settings, as well as experimentation or test and evaluation, providing design understanding of CEMA activities in an M&S environment can avoid unintended consequences, such as interruption of non-military spectrums, networks, computers, or communications systems. To manage representing these challenges in M&S, one can separate activities into "Cyber for Cyber" and "Cyber for Others"[2] in the case of the cyber component. (Although one could make a case that this could be "CEMA for CEMA" and "CEMA for Others.") But since CEMA, especially the cyber portion, is nearly omnipresent across MDO, the "Cyber for Others" is critically important for interfacing with command staffs and operational units. Although the Army has joined cyber with EW and spectrum management operations (SMO) into the concept of CEMA as a doctrinal organizing term (Headquarters, Department of the Army, 2014), the connection between cyber and EW/SMO is not always readily apparent. MDO includes cyberspace as well as EW-critical enabling capabilities, and understanding how CEMA impacts MDO provides opportunity, that almost necessitates a use for M&S to gain insights about the connections across CEMA and the impacts of their effects.

M&S opportunities to create understanding in MDO are plentiful. 1) Consider the long history of distributed simulation standards that has evolved to solve the problem of kinetic M&S interoperability. Much of this history has been dedicated to finding suitable data exchange models between kinetic simulations developed at different times for different purposes, and for different M&S communities within the Army. The opportunity exists today to minimize the interoperability issues for CEMA M&S, particularly energized by the emergence of MDO and CEMA doctrine. A framework such as the CEMA M&S Framework (CMFW) can help the systemization of non-kinetic M&S for CEMA, thereby increasing the ability of different M&S instances to interoperate in more meaningful ways. 2) A CMFW can also assist in M&S gap identification (Army Modeling & Simulation Office, 2021) for M&S practitioners and developers. To address the lack of an organizing approach, such as a framework, this CMFW provides M&S developers with a common reference, doctrinally based, and operationally informed for unclassified collaboration. This can enable dialog with operational users of CEMA that can lead to an understanding to further shape appropriately classified M&S applications, data, and services. 3) Finally, the increased awareness and opportunity for education across the force about how to approach CEMA tasks while using M&S is of paramount importance.

ASPECTS OF MDO

Multi-Domain Operations (MDO) is the consolidating concept of the US Department of Defense (DoD) for future military operations and consists of kinetic and non-kinetic effects across the domains of Land, Maritime, Air, Space, and Cyberspace. Joint Publication (JP) 3-0 describes the operational environment across the conflict continuum and the range of military operations that can be executed. The physical domains of Air, Land, Maritime, and Space are impacted by the information environment which includes cyberspace and the electromagnetic spectrum. Additionally, JP 5-0 (Joint Staff, 2011) provides an integrated perspective of cyberspace's impact in the physical domains as represented in Figure 1.

[2] The terms Cyber for Cyber and Cyber for Others denote a distinction between personnel whose main mission is cyber-related (Cyber for Cyber) whereas Cyber for Others is a term that refers to the need for all personnel in every operational mission to be aware of and trained in cyber-related concepts.

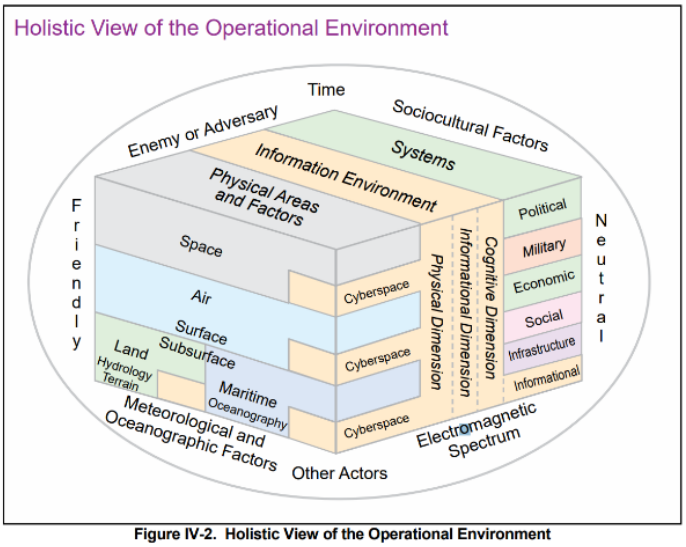

Figure IV-2. Holistic View of the Operational Environment

Figure 1. JP 5-0 Holistic View of the Operational Environment

The global domain of cyberspace connects and integrates the four physical domains (land, air, maritime, and space) within the folds of the information environment (Bates). Cyberspace bridges the physical and cognitive worlds in a manner that constructs an operational environment (Joint Staff, 2011) where MDO is executed.

Figure 2 shows one way in which MDO concepts can be translated into a Unified Modeling Language (UML) representation and associated with the Army Futures Command (AFC) Cross Functional Teams (CFTs). MDO attempts to address the five operational problems for the Joint Force as presented in TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028 (Battlefield Development Plan Branch, Joint & Army Concepts Division):

(1) How does the Joint Force **compete** to enable the defeat of an adversary's operations to destabilize the region, deter the escalation of violence, and, should violence escalate, enable a rapid transition to armed conflict?
(2) How does the Joint Force **penetrate** enemy anti-access and area denial systems throughout the depth of the Support Areas to enable strategic and operational maneuver?
(3) How does the Joint Force **dis-integrate** enemy anti-access and area denial systems in the Deep Areas to enable operational and tactical maneuver?
(4) How does the Joint Force **exploit** the resulting freedom of maneuver to achieve operational and strategic objectives through the defeat of the enemy in the Close and Deep Maneuver Areas?
(5) How does the Joint Force **re-compete** to consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?

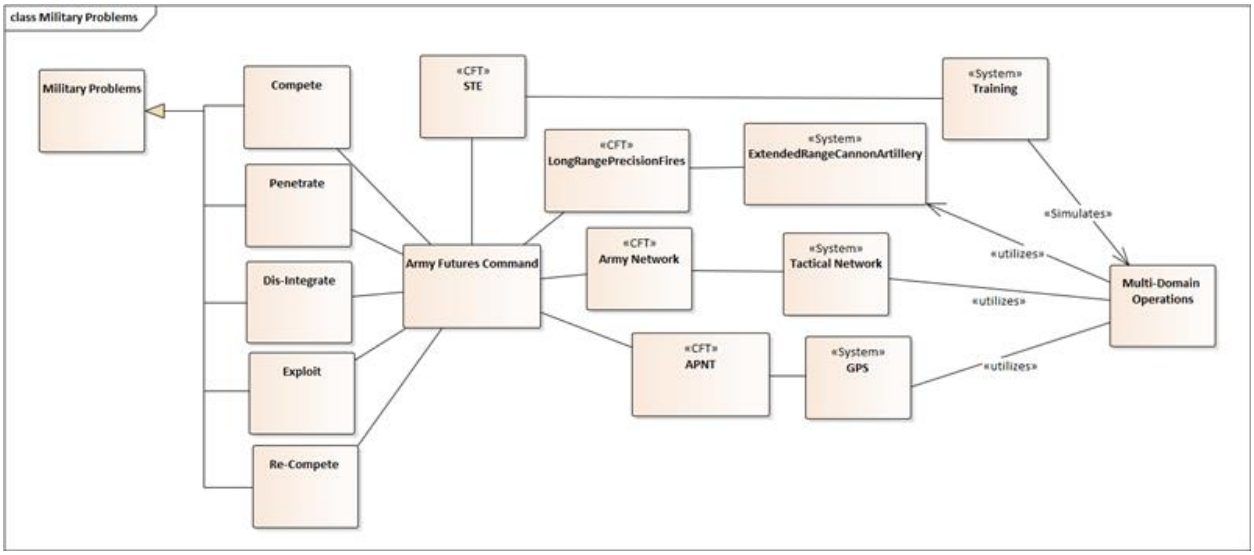

Figure 2. Partial representation (extract from CMFW) of the relationship of MDO to AFC and the CFTs

The Army's response to MDO is guided by the Battlefield Development Plan (BDP) which identifies the requirements to support MDO across the areas of doctrine, organization, training, material, leadership and education, personnel, facilities, and policy (DOTMLPF-P). The BDP process cycles align with Total Army Analysis (TAA) and Program Objective Memorandum (POM) budget cycles in an iterative manner to ensure a holistic approach for modernization (Wilson, Farrell, Jacobsen, & Owens, 2020). The five problems above are addressed in the BDP and solution concepts presented by echelon (Battlefield Development Plan Branch, Joint & Army Concepts Division).

To address the materiel area aspects of the five problems the US Army identified CFTs to develop systems and platforms that would focus on capabilities needed for successful MDO: 1) Long Range Precision Fires (LRPF); 2) Network; 3) Advanced Positioning, Navigation, and Timing (APNT); 4) Future Vertical Lift; 5) Air and Missile Defense; 6) Next Generation Combat Vehicle (NGCV); 7) Soldier Lethality; and 8) Synthetic Training Environment (STE). These CFTs consist of all the development components needed to deliver a material solution in the shortest time possible. Initially, these CFTs were standalone organizations. But shortly after establishing them, the US Army created a headquarters element and inaugurated the Army Futures Command (AFC) to support coordination across the CFTs and with the rest of the Army. The systems and platforms being developed by the CFTs will be utilized by commanders in the conduct of MDO, except the STE, which will simulate the MDO environment to assist forces in preparing for combat. The authors used this MDO construct for the CFTs to develop mission threads to identify the CEMA aspects of CFT efforts and integrate them with the previously developed CEMA M&S Framework.

Importance of CEMA to MDO

Our military forces rely upon network connectivity for the information environment required to complete command, control, and communications (C3) tasks. Both Joint and Army doctrine have for some time recognized the integrated nature of cyberspace and the interrelationship of kinetic and non-kinetic effects. This pre-MDO viewpoint has expanded to an explicit domain within MDO that must be considered when executing military operations. The Army's CEMA concepts support the Joint perspectives and drive the actions to mature the M&S needed to support CEMA. This operational environment is the composite of these domains where conditions, circumstances, and influences affect the employment of military force decision-making and capabilities. Access to this interconnectivity by the military to communicate, conduct operations, and to meet the nation's objectives (Bates) across multiple domains.

Combining the previously mentioned JPs with recent discussions (Headquarters, Department of the Army, 2021) has highlighted MDO aspects in the continuum from competition to conflict. The authors have observed the CEMA overlaps in this continuum as illustrated in Figure 3, which illuminates its ubiquity.

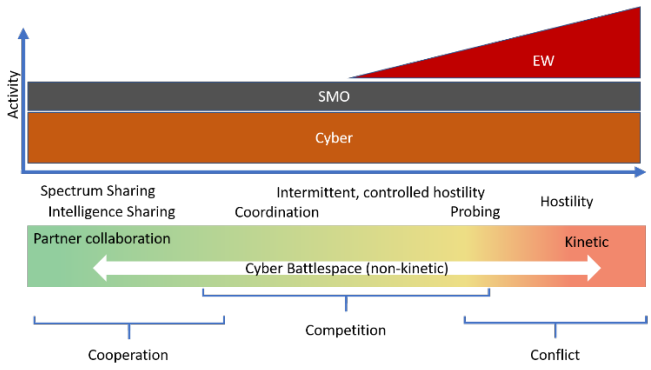

Figure 3. CEMA in the cooperation to conflict continuum

As seen in the previous figures, the extensive impact of the non-kinetic cyber battlespace on the range of military operations within the MDO construct drives the need to express CEMA in M&S capabilities. The out-sized bearing of CEMA across all domains and all military operations requires a correct representation of CEMA effects in M&S. Failing to do so hampers the ability of Army forces to be fully prepared to accomplish their assigned missions.

The authors used a deliberate design to enhance the CMFW by gaining an understanding of non-kinetic cyber battlespace characteristics through operational mission threads that capture the CEMA components within common operational scenarios closely aligned to CFT acquisition activities.

RESULTS AND FINDINGS

We introduce some basic concepts about modeling CEMA in an MDO context. We discuss some basic concepts required for modeling CEMA and especially for modeling CEMA within an MDO context.

Modeling CEMA for MDO

We address three levels or aspects of CEMA modeling concepts: 1) ontologies; 2) system modeling and data exchange; and 3) mission threads. The first of these, ontologies, provides several broad perspectives of the entire domain of CEMA. The second, system modeling, examines how a modeler might represent the CEMA aspects of an individual system (e.g., a missile or vehicle). The data exchange portion of the CMFW incorporates and references the ongoing work of the Simulation Interoperability Standards Organization (SISO) Cyber Data Exchange Model (DEM) working group (Simulation Interoperability Standards Organization, n.d.). The third aspect begins to tie the first two views together in an operational context by illustrating some typical system supported mission threads that would be executed within the MDO context. Having this framework reference can enable code discovery and reuse, unlike the stove-piped development of kinetic models and simulations of the past five decades. We continue to build on previous work (Vey, et al., 2019). The CMFW was originally constructed with three interrelated ontologies: a High Level Ontology, a Doctrinal Ontology, and a Technical Level Ontology. In addition, the framework had components of architecture and code. The current structure of the CMFW is shown in Figure 4 as it appears in our Enterprise Architect modeling tool.

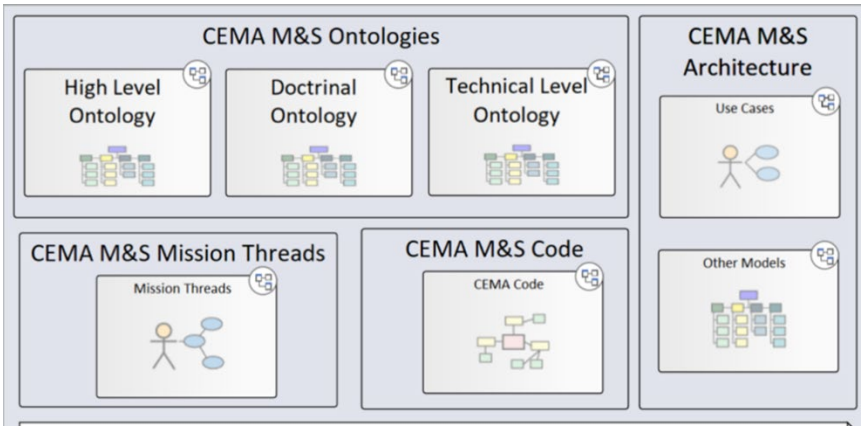

Figure 4. CMFW Top Level Structure

Reviewing the three current ontologies that comprise the CMFW, the high-level ontology provides an operational view of CEMA, illustrates the similarities between Cyberspace Domain Activities and traditional domain activities; the doctrinal ontology is based on the U.S. Army's CEMA Field Manual (Headquarters, Department of the Army, 2017); and the technical ontology maps these concepts into the M&S space. The relationship of these ontologies is shown in Figure 5. We discuss our results and findings first in terms of how CEMA relates to MDO in both Joint and Army contexts. Then we show examples of how simple modeling techniques can shed light on MDO through M&S and conclude with connections between CEMA and Digital Engineering.

CMFW Ontologies

The detailed ontologies referenced in Figure 4 do not lend themselves to full representation in this paper format, but Figure 5 shows one way in which the ontologies tie together and serve to provide context and information about CEMA relationships.

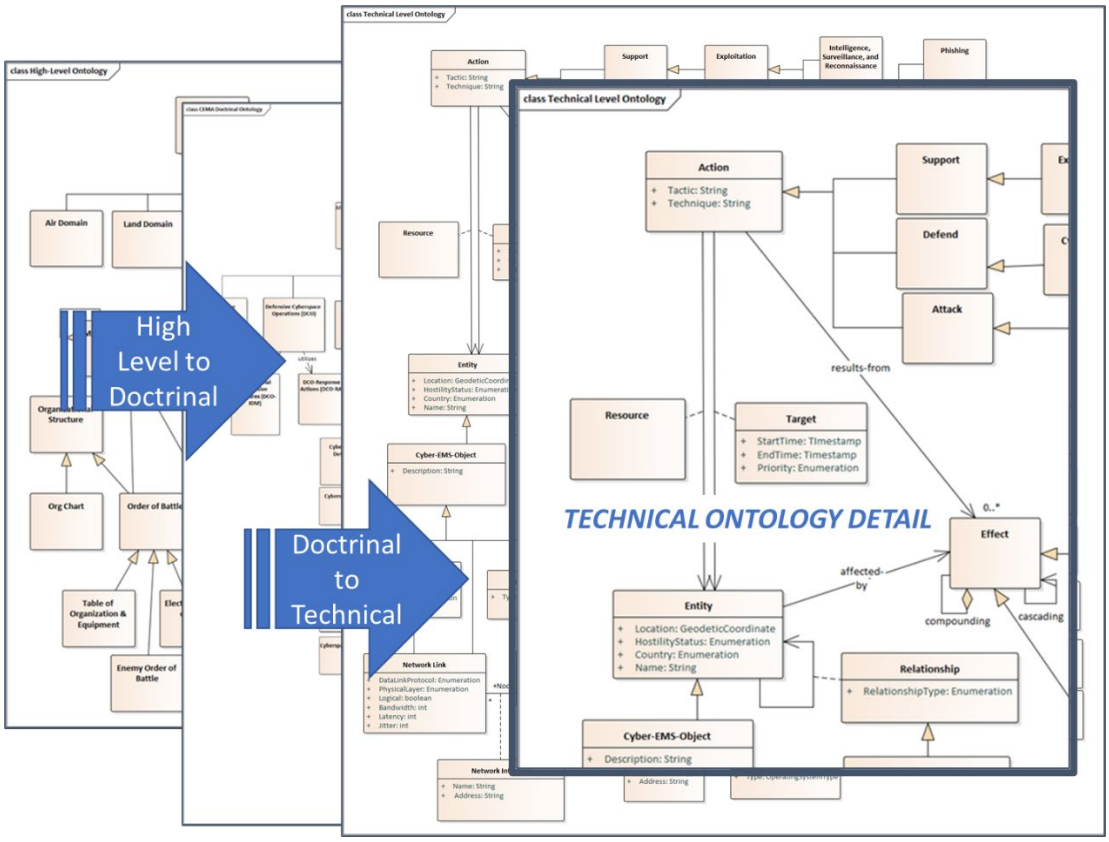

Figure 5. CMFW Ontologies

The bottom layer of Figure 5 depicts the High Level Ontology providing a broad view of CEMA; the next level shows the Doctrinal Ontology; the top level shows the Technical Ontology. The Technical Ontology can also be thought of as the M&S ontology. The top panel of this figure shows a detail from the Technical Ontology.

Systems Models and Data Exchange Models

To accommodate the potential need to model systems explicitly within MDO, we have included a generic model of a cyber-physical system (CPS) (National Institute of Standards and Technology, n.d.). As Figure 6 shows, such a generic system is composed of components which may have CEMA attributes. Prominent categories of attributes include those indicated in the figure: computing, interface, storage, sensor, actuator, EMS receiver and emissions.

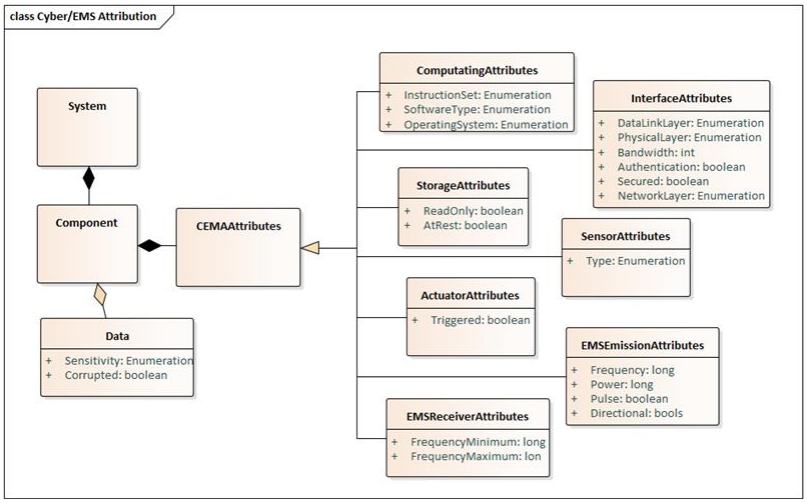

Figure 6. A Generic Model of a CPS with Attribution

Incorporating Electronic Warfare and Spectrum Management Operations

Figure 7 is a representation of Electromagnetic Spectrum Operations (ESO). This portion of the ontology depicts ESO in a conventional manner with both Electronic Warfare (EW) and Spectrum Management

Operations (SMO). The ontology also highlights the presence of spectrum dependent devices (SDD) within the Electromagnetic Operational Environment. From a modeling perspective, an analogy can be drawn between the Electromagnetic Operational Environment and conventional "terrain." In addition, the concept of the SDD in ESO is analogous to a CPS in the purely cyber domain.

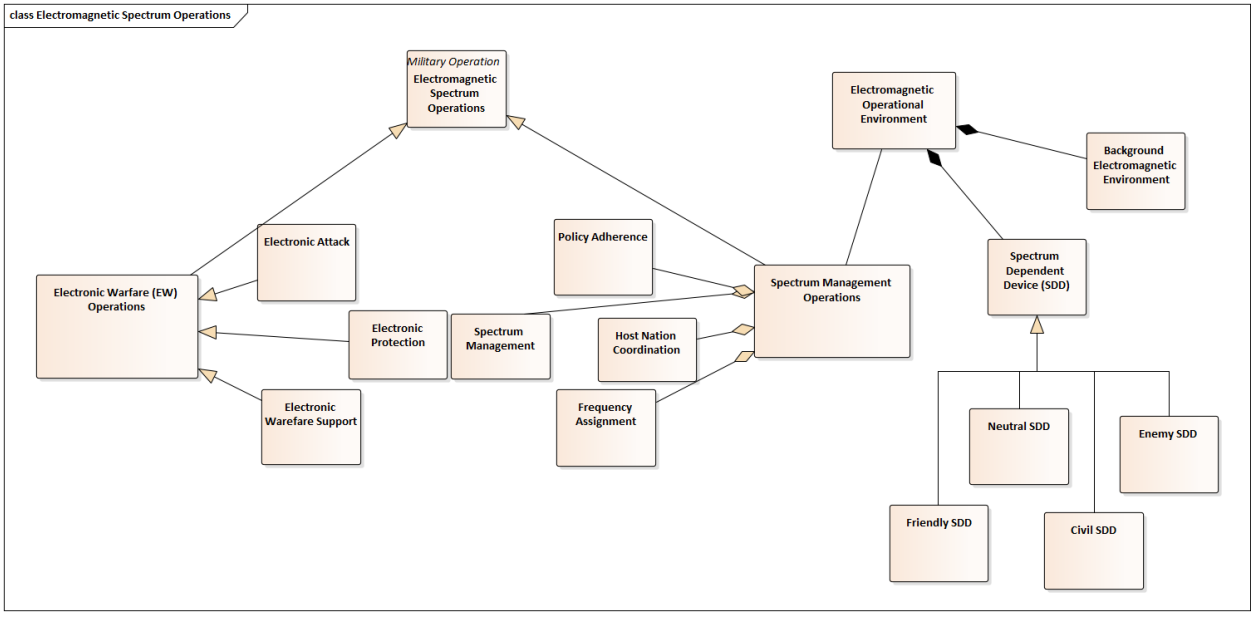

Figure 7. Electromagnetic Spectrum Operations and EMS Operational Environment/Spectrum Dependent Devices

Mission Thread Examples for Cross Functional Team (CFT) Problem Spaces

The relationship between the U.S. Army's concepts of CEMA and MDO is complex. Cyberspace activities, incorporated as part of CEMA, have had several decades of exponential growth due to computing and network technology capabilities that have enabled cyberspace weaponization and have blurred the boundaries between competitive commerce and hostile actions. The cyberspace domain is one of the greatest enablers of MDO, yet it also provides opportunities for exploitation (Bates). Our team took the high level MDO objectives for CFT-developed systems and platforms and decomposed them into Mission Threads to tease out the CEMA related effects or capabilities inherent in the CFT's efforts.

The CMFW team consists of both military subject matter experts (SME) as well as technologists. Collaboration within our team involved the use of different tools and techniques. The CMFW team considered AFC CFT capabilities that could be impacted by CEMA to address the challenges of MDO (Army Futures Command, n.d.) that M&S must consider. This mission thread approach fills the space between CFT and MDO shown in Figure 2 above and describes how CFT products may be used in MDO while teasing out the CEMA implications.

Our team uses UML as the foundation for the CMFW to support future efforts in Digital Engineering and system/software engineering. The authors also leveraged the ArchiMate modeling notation for portions of its mission thread effort. ArchiMate is the preferred mission thread notation of the North Atlantic Treaty Organization (NATO) using NATO Architecture Framework version 4 (NAFv4) viewpoints (North Atlantic Treaty Organization (NATO), 2020).

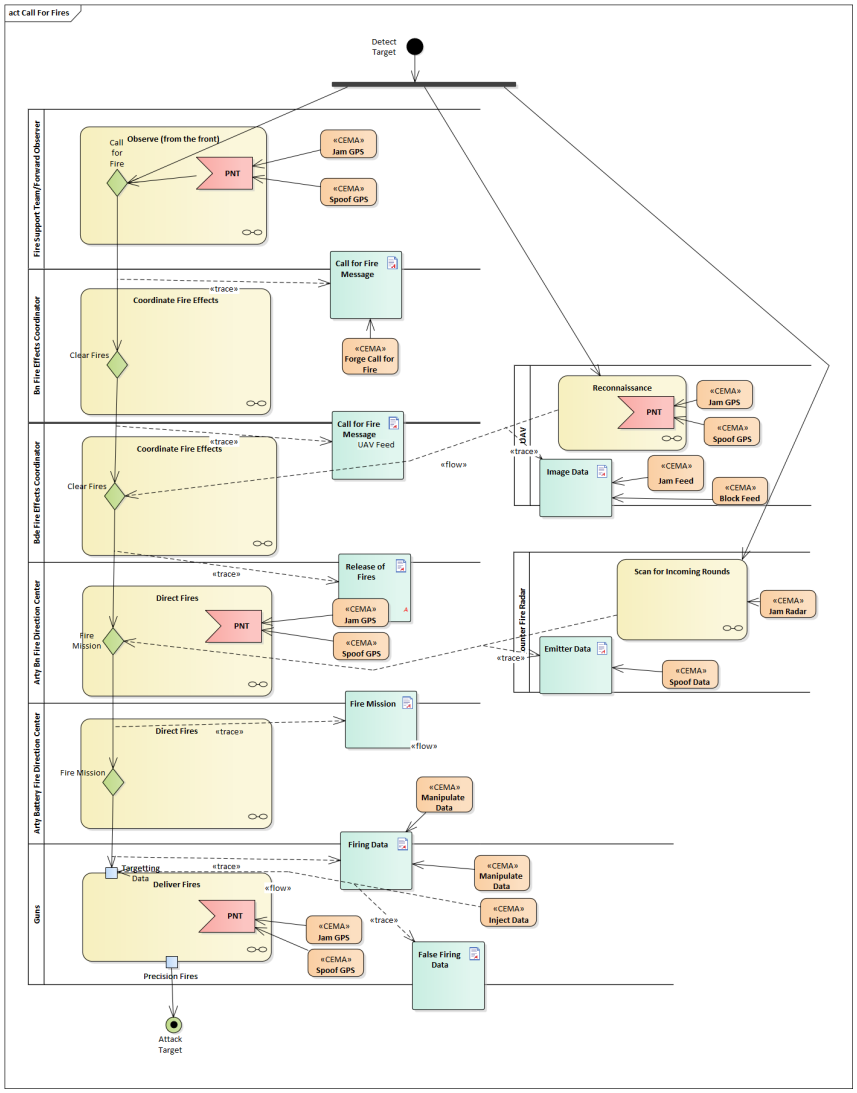

Figure 8. Generic Call for Fire CEMA M&S Mission Thread: Concept to Diagram

Generic Call for Fires Mission Thread Example. As an example of how CEMA M&S might impact the Long-Range Precision Fires (LRPF) CFT, the CMFW team built a generic "call for fires" mission thread depicted in Figure 8. The mission thread details how observed fires are conducted and shows the potential for CEMA effects to impact any call for fires mission that uses electronics, cyber physical systems (CPS), or transmitting or receiving electromagnetic equipment.

This diagram uses a stack of swim lanes representing military units or functions such as a Fire Support Team. Each swim lane contains activities with highlighted CEMA components such as a positioning, navigation, and timing (PNT) element. Potential vulnerabilities are identified from target location error (TLE), communications methods, and even through the powder temperature probe.

Generic NGCV MTC Mission Thread Example. As another example (Figure 9), we developed a concept model of how CEMA might be a factor in a movement to contact (MTC) type of mission using a modern ground vehicle such as the next generation combat vehicle (NGCV), the focus of one of the AFC CFTs. The thread outlines how CEMA could be embedded into a NGCV equipped force as it conducts a non-kinetic MTC to determine threat cyber, EW, and SMO locations and capabilities. This is a significant departure from the Army's description of a kinetic-based MTC operation to regain contact with an enemy force (Headquarters, Department of the Army, 2019) and points to the ever-evolving nature of military operations when confronted with CEMA components.

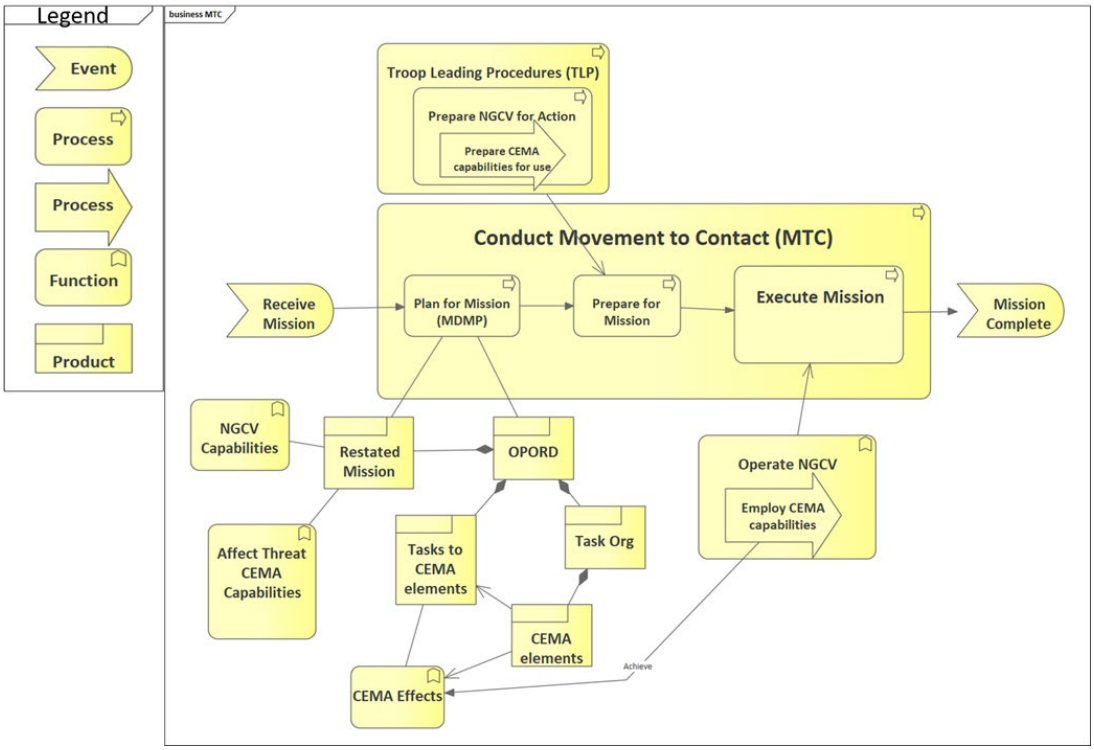

Figure 9. CEMA Impact on MTC Mission with Ground Vehicle

Generic Future Vertical Lift (FVL) Mission Thread Example. A mission thread has also been developed that considers the end-to-end activities associated with the release of the Air Tasking Order (ATO). Once the ATO is provided to Aviation units, the unit begins planning with the Air Mission Planning System (AMPS) then uploads mission data into the airframe platform flight computers. The aircraft then flies the mission and reports for a debrief. The diagram (not shown) identifies the information systems and cyber physical systems (CPS) along with the information exchanged and the CEMA interaction points to identify potential vulnerabilities. During ATO related activities, adversary CEMA could modify the ATO itself, impact the digital maps used in planning, influence the flight weather data, affect the digital and non-digital components of the aircraft during manufacture, suppress navigation signals during execution, and similar CEMA effects.

Generic Advanced Positioning, Navigation, and Timing (APNT) Mission Thread Example. Underpinning our combat platforms and C2 systems are the PNT assets that encircle the planet. Across the globe, all weapon systems, platforms, sensors, and communication networks rely upon the capabilities of this information network (TRADOC, 2018) to accurately identify their location, threat locations, and munitions *en route* to targets while synchronizing operations across all domains. This mission thread is in development and will outline the potential CEMA actions that adversaries could take that can impact MDO.

Mission Thread Summary. In each mission thread, the CEMA element is tagged with potential CEMA actions, either offensive or defensive. We found that simply modeling a generic mission thread in this manner exposes many areas of potential vulnerability, some expected, others unexpected. These generic mission threads can serve as reference models for specific systems and missions. Similar mission threads for generic representations of other CFTs are under development.

Supply Chains and CEMA M&S

Recent events (New York Times, 2021) (New York Times) (Reuters) have highlighted the importance of the supply chain and other commercial vulnerabilities in national and global critical infrastructure. We have added a simple supply chain model to the CMFW (Figure 10) as a recognition of its growing importance in the continuum of cooperation to conflict (see Figure 3). This model is based on commercial models (North Carolina State University, 2021) (Box Around the World, n.d.). It models a process from its origin at a supplier into a product through logistics and operation.

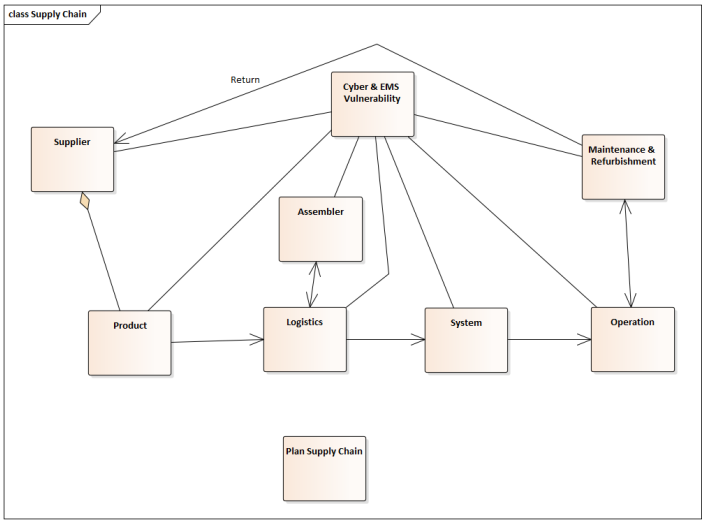

Figure 10. A Simple Supply Chain Model

CEMA, MDO, and Digital Engineering

The pervasive nature of the cyber battlespace across all domains indicates that it must be accounted for at the earliest possible point in the acquisition cycle. The DoD recognizes this fact (Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2018) and is re-emphasizing its Digital Engineering (DE) efforts to leverage M&S to support the development of system capabilities. The Army's CEMA capabilities and concepts must be captured and applied where appropriate within DE to ensure vulnerabilities are mitigated and capabilities are enhanced to the detriment of threat operations. The CMFW, particularly with the development of mission threads and updates to the ontologies, deliberately approached development as informed by engagement with DoD DE strategy and guidance so that this effort can serve to advance those concepts and approaches for development of other M&S tools and services.

RECOMMENDATIONS

The CMFW remains a work in progress, and we believe the M&S, CEMA, and MDO communities will benefit from continued maturation. In addition, and more specifically, based on our work using the CMFW to explore MDO concepts, we make the following recommendations:

1. Continue to update the CMFW to remain consistent with doctrine, lessons learned by operational forces and developments with CEMA M&S tools, services, and data. Work with other services, across DoD, to account for CEMA as applicable for MDO.
2. Develop requirements and M&S tools to represent CEMA effects modeling to address operational campaign understanding for readiness strategy, force design and development activities.
3. Use the CMFW as a basis to develop an CEMA MDO Playbook for M&S Development to enable operational CEMA users with an understanding of CEMA and implications of working with CEMA-related M&S tools.
4. To deepen the utility and connection with Digital Engineering, we recommend using Model Based Systems Engineering (MBSE) methods, especially the use of SysML to transform the UML-based CMFW to a true Digital Engineering product.
5. Based on these and similar models, simulations need to incorporate the visualization of the electromagnetic spectrum, interference, jamming, internet service providers, cell towers, routers, and networks.

SUMMARY

The CMFW effort provides a common reference framework and architectural ontology to enable development of M&S that encompass non-kinetic factors that exist to prepare for the MDO environment. Particularly this project delivers a framework that contains mission threads developed from Army Cross Functional modernization efforts with deliberate focus on a common reference for the non-kinetic challenges of representing CEMA in simulations tools. Having this as current developers work to represent the numerous M&S gaps faced by Army communities of interest (acquisition, analysis, intelligence, test and evaluation, experimentation, and training) as well as the challenges in the broader Joint and DoD communities, provides a guiding reference for non-kinetic effects M&S development. Simulations need to accurately portray CEMA, C2 assets, and networks across all M&S domains in support of those various standards and fidelity requirements. This simulated environment provides the human warrior an opportunity to be prepared for the future operational environment (TRADOC, 2018). The framework serves to establish common understanding now as we invest in our requirements to deliver MDO.

ACKNOWLEDGEMENTS
The authors would like to acknowledge funding support for this research from the Army Modeling and Simulation Office (AMSO). The authors would also like to acknowledge individuals and organizations throughout the DoD community who have taken the time to provide comments on this work. The authors would like to acknowledge the SISO Cyber DEM team, led by Dr. Katherine Morse.

REFERENCES

Army Futures Command. (n.d.). Retrieved May 6, 2021, from Army Futures Command: https://armyfuturescommand.com/

Army Modeling & Simulation Office. (2021). *Cyber and EW M&S Gaps Working Papers.* CyEWMSWG.

Army Modeling and Simulation Office. (2021). AMSO Annual Gap Forum. *CyEWMSWG Gaps*. Ft Belvoir.

Bates, C. (n.d.). Preparing for the All-Domain Battlefield. *Aerospace & Defense Review*. Retrieved May 24, 2021, from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JA-20/Executive-Summary-The-Battlefield-Development-Plan-2019-Finalv2.pdf

Battlefield Development Plan Branch, Joint & Army Concepts Division. (n.d.). *Executive Summary: The Battlefield Development Plan 2019: Field Army, Corps, & Division in Multi-Domain Operations 2028.* Retrieved May 21, 2021, from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JA-20/Executive-Summary-The-Battlefield-Development-Plan-2019-Finalv2.pdf

Box Around the World. (n.d.). *Supply Chain Modeling 101! Understanding the Different Types of Supply Chain*. Retrieved June 28, 2021, from boxaroundtheworld.com: https://boxaroundtheworld.com/supply-chain-modeling-101/

Department of the Army. (April, 2017). *FM 3-12, Cyberspace and Electronic Warfare.*

Headquarters, Department of the Army. (2014). *FM 3-38 Cyber Electromagnetic Activities.* Washington, D.C.: U.S.Army.

Headquarters, Department of the Army. (2017). *Cyberspace and Electronic Wafare Operations.* Department of the Army.

Headquarters, Department of the Army. (2019). *Army Doctrine Publication (ADP) 3-90 Offense and Defense.*

Headquarters, Department of the Army. (2021). *Army Multi-Domain Transformation, Ready to Win in Competition and Conflict.* U.S. Army. Retrieved from https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf

Joint Staff. (2011). *Joint Publication 5-0, Joint Operation Planning.*

National Institute of Standards and Technology. (n.d.). Retrieved June 10, 2021, from Cyber-Physical Systems: https://www.nist.gov/el/cyber-physical-systems

New York Times. (2021). Colonial Pipeline chief says an oversight let hackers into its system. *New York Times*. Retrieved June 10, 2021, from https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

New York Times. (n.d.). Ransomeware Disrupts Meat Plants in Latest Attack on Critical U.S. Business. *New York Times*. Retrieved June 10, 2021, from https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html

North Atlantic Treaty Organization (NATO). (2020). *Implementing NATO's Mission Thread CAPSTONE Concept: Stype Guide for Modelling in Archimate, Architecture Capability Team(ACT) Consultation Command and Control Board (C3B).*

North Carolina State University. (2021). *The SCOR Model for Supply Chain Strategic Decisions*. Retrieved from Supply Chain Resource Cooperative: https://scm.ncsu.edu/scm-articles/article/the-scor-model-for-supply-chain-strategic-decisions

Office of the Deputy Assistant Secretary of Defense for Systems Engineering. (2018). *DoD Digital Engineering Strategy.* Department of Defense.

Reuters. (n.d.). SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president. *Reuters.com*. Retrieved June 10, 2021, from https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R

Simulation Interoperability Standards Organization. (n.d.). *Cyber DEM PDG - Cyber Data Exchange Model*. Retrieved May 6, 2021, from SISO: https://www.sisostds.org/StandardsActivities/DevelopmentGroups/CyberDEMPDG.aspx

The Joint Staff. (2017 with Change 1, 2018.). *Joint Publication 3-0, Joint Operations, .*

TRADOC. (2018). *The U.S. Army in Multi-Domain Operations 2028, TRADOC Pamphlet 525-3-1.*

Vey, N., Heidelbaugh, C., Friest, T., Ruth, J., Bates, C., & Riecken, M. (2019). A Cyberspace and Electromagnetic Activities (CEMA) Framework for M&S.

Wilson, B., Farrell, D., Jacobsen, T., & Owens, J. (2020). The Battlefield Development Plan: A Holistic Campaign Assessment to Inform the Army Modernization Enterprise. *Military Review*.