Contextualizing Cyberspace Electromagnetic Activities (CEMA) in Multi-Domain Operations (MDO) Through Playbooks

COL Chad Bates, Ph.D.
US Army War College
Carlisle, PA
chad.t.bates.mil@mail.mil

Dr. Jacob Cox, Mr. Clark Heidelbaugh,
Mr. Jim Ruth, Mr. Tim Friest,
Trideum Corporation
jcox@trideum.com, cheidelbaugh@trideum.com,
jruth@trideum.com, tfriest@trideum.com

ABSTRACT

Modern warfare mandates that adversaries have the ability to engage one another in Multi-Domain Operations (MDO) that span land, maritime, air, space, and cyberspace. To do so effectively, warfighters must not only integrate an array of capabilities, but also synchronize Cyberspace Operations (CO) and Electromagnetic Warfare (EW) across all domains and lines of operations to gain information advantage. Commanders and staff must understand CO, EW, and other military capabilities (e.g., intelligence, signal, information advantage activities, and fires) and how they can be integrated to support operations. As defined in FM 3-12, this integration occurs through cyberspace electromagnetic activities (CEMA). However, this is an area of simulations and training that is searching for a viable solution to allow units to accurately develop a realistic MDO environment.

Doctrine reveals very little about how commanders and staff should envision CEMA tactics and actions, how CEMA can be synchronized with kinetic operations, or how enemy actions will affect their communications and other systems. This gap creates a training environment where warfighters struggle to visualize the operational environment through the lens of CEMA. As an initial step to addressing this challenge, we developed a CEMA MDO Playbook for training events and simulations that demonstrates how cross-domain capabilities, such as EW, CO, maneuver, and fires, can introduce dilemmas for the enemy while enabling friendly forces to conduct operations in degraded, disrupted, and/or denied operational environments.

The Playbook can also assist teams to create training exercises or Modeling & Simulation (M&S) events with CEMA effects by integrating known simulations with plays from a common reference booklet. In the future, we envision a playbook supporting visual mappings of multiple battlefield entities, encompassing different activities (CO and EW), actions, and impacts within training simulations and other events.

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 Cyber Warfare Officer (Branch Specialty 17) and Modeling and Simulation Officer (Functional Area 57) for over 18 years within his 28-year career. He is currently assigned as a Cyber / Wargaming Research Professor, at the United States Army War College. Prior to this assignment, COL Bates served with the U.S. Army Cyber Command (ARCYBER), and within the Deputy Chief of Staff for Intelligence (DCS G-2) as an M&S expert for Cyber and 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.

Dr. Jacob Cox is a solutions architect (cybersecurity and EW) for Trideum Corporation and an adjunct professor in the School of Computer and Cyber Sciences at Augusta University, GA. Dr. Cox' previous positions include research scientist in an artificial intelligence research company, focusing on cybersecurity, and lead data scientist for Army Capability Manager – Cyber, researching cyberspace situational understanding technologies for MDO. Dr. Cox has over 22 years of U.S. Army service in both technical and operational assignments, serving as a signal officer, a

telecommunications engineer, and cyber operations officer. He holds a B.S. degree from Clemson University in Electrical Engineering. He also holds an M.S. degree from Duke University and a Ph.D. from Georgia Institute of Technology, both in Electrical and Computer Engineering. His certifications include CISSP, PMP, CEH, and CHFI. He is a contributor to the CEMA MDO playbook and to use case development for CEMA capabilities in MDO for operational tests.

Mr. Clark Heidelbaugh works with Cyberspace and Electromagnetic 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 an MS in Systems Engineering, an MS in OR, a Master of Strategic Studies-Advanced Strategic Art Program, 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 Electromagnetic 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.

Contextualizing Cyberspace Electromagnetic Activities (CEMA) in Multi-Domain Operations (MDO) Through Playbooks

COL Chad Bates, Ph.D.
US Army War College
Carlisle, PA
chad.t.bates.mil@mail.mil

Dr. Jacob Cox, Mr. Clark Heidelbaugh,
Mr. Jim Ruth, Mr. Tim Friest
Trideum Corporation
jcox@trideum.com, cheidelbaugh@trideum.com
jruth@trideum.com, tfriest@trideum.com

INTRODUCTION

Future Army operations will engage adversaries across all domains—land, sea, air, space, and cyberspace—during competition, armed conflict, and return to competition phases of Multi-Domain Operations (MDO). While four of these domains are defined by the space they inhabit, cyberspace is the domain that exists within all others. However, how operations in and through the cyberspace domain converge with operations across the other domains is still not well defined or understood.

For instance, U.S. Army doctrine, TRADOC Pamphlet (TP) 525-3-1, The U.S. Army in Multi-Domain Operations 2028 (2018), requires Army forces to enable and complement land, air, and maritime capabilities with operations in space, cyberspace, and the Electromagnetic Spectrum (EMS) to support the opening of and exploitation of windows of superiority. In MDO, these windows create dilemmas for the enemy while protecting the friendly force's ability to conduct operations in degraded, disrupted, or denied operational environments. The ability of Army formations, at each echelon, to converge capabilities in multiple ways and sequences also provides the Joint Force Commander with options to impose additional complexity on the enemy. Such efforts require coordination through cyberspace, making Cyberspace Electromagnetic Activities (CEMA) foundational to MDO and multi-national operations.

CEMA, as defined in FM 3-12, Cyberspace Operations and Electromagnetic Warfare (2021), is the Army's process of planning, integrating, and synchronizing cyberspace operations and electromagnetic warfare. It links CEMA with aspects of the MDO found in TP 525-3-1, such as the information environment operations (IEO). IEO is the integrated employment of information-related capabilities (IRC) in concert with other lines of operation. These capabilities influence, deceive, disrupt, corrupt, or usurp the decision-making of enemies and adversaries while protecting friendly access to the same. FM 3-12, while linking CEMA and IEO, also lists cyberspace operations and EW effects as IRCs.

This connection is additionally found in a 2020 paper (Fogarty & Sparling, 2020) where the authors observe that CEMA is expanding to include all aspects of IEO. In their paper, they wrote, "current Cyber-Electromagnetic Activities (CEMA) cells will expand to include increased IO [Information Operations], PSYOP [Psychological Operations], and Public Affairs personnel, and upgraded capability packages to improve tactical commanders' information capabilities" (p. 24). Doing so aligns the Army's IEO with Operations in the Information Environment (OIE) used by Joint community and sister services. OIE, for instance, includes civil-military operations, disinformation, propaganda, narrative warfare, and other capabilities seen as belonging to IEO in the Army's MDO doctrine.

As of 2021, FM 3-12 states that "ARCYBER also integrates intelligence, fires, space, psychological operations, strategic communications, public affairs, special technical operations, cyberspace operations, electromagnetic warfare, and information operations to allow Army commanders a decisional advantage during competition and conflict" (p.3-1). While CEMA provides the avenue for converging cross-domain capabilities, the skills and insight needed to prepare tactical (Division and below) commanders—those in "CEMA-for-Others" positions[1]—to employ cross-

[1] The distinction we hold to in this paper is that CEMA-for-Others supports warfighters (commanders and staff) who do not hold positions directly related to cyber, EW, IO, and others listed in this paper. They focus on leveraging CEMA capabilities to accomplish their mission, but not the actual deployment of these capabilities; therefore, they must understand the effects these systems will create.

domain capabilities is lacking. They must learn about, train with, employ and generally experience the capabilities that exist and will exist with CEMA.

The task we must address is this—how do we prepare warfighters to leverage CEMA to execute convergence and cross-domain maneuvers to see, isolate, maneuver, and/or protect to exploit the initiative and achieve positions of advantage to accomplish their missions? Especially if this is an environment where very few have experience, and the technology is rapidly being improved and integrated into operations. Resources are needed, both to enhance training and to inform modeling and simulation (M&S) development. This paper not only serves to provide the cognitive framework of how MDO operations could be conducted through playbooks but also offers concrete examples of how they may be implemented in training and simulation environments. Hence, the CEMA MDO Playbook incorporates concepts, mission threads, plays, and processes to allow tactical commanders and staff to understand and employ CEMA in MDO to enhance their capabilities. Visual mappings of battlefield activities/actions/impacts are also included to better enable the creation of realistic simulations or Mission Scenario Event Lists (MSELs) to support training and testing.

BACKGROUND

In 2012, researchers at the United States Military Academy articulated how global positioning system (GPS) satellites guide troops and weapon systems, algorithms fly aircraft and allocate supplies, and computer networks almost exclusively facilitate the transfer of official and personal data and voice communications (Brickey et al., 2012). Their goal was to offer a compelling case for cybersecurity, garner support, and motivate action within the military by citing real-world cases with military applications. They pointed to Iran's capture of a US drone by jamming its GPS guidance system and how the Air Force discovered a virus in the remote cockpits of its drone fleet. Their article also addressed the need for training cybersecurity but fell short of offering how it might be simulated in a training event.

Fast forward to today, and the U.S. Army has seen two decades of fighting counterinsurgency where it had superiority in communications and network infrastructure. U.S. Forces have tremendous experience where the network is always operational, having established redundant operating bases and reliable communication networks over these years. However, in Large Scale Combat Operations (LSCO) with a peer adversary, the #1 target will be the network since it is a foundational weapon system to the U.S. military and its allies for employing firepower on the battlefield. Additionally, U.S. analyst predict peer adversaries will develop novel asymmetric capabilities that place our joint forces at significant risk of being outflanked in competition and enabling their fracture and disintegration by 2040 (McConville, 2021).

U.S. leaders are seeking to implement a 21st-century talent management system, develop and field new weapon systems, transform its doctrine, build new organizations, and change the way the U.S. Army trains (McConville, 2021). All of this is done within the concept of MDO, which was officially adopted as a significant doctrinal "inflection point" in the Army's October 2022 release of Field Manual (FM) 3-0, Operations. MDO represents a shift from the past two decades of Counter Insurgency Operations (COIN) to a renewed focus on LSCO and near-peer threats. To support the Joint Force in MDO and win the next fight, the Army's transformation must offer the range, speed, and convergence of technologies that are needed to achieve future decision dominance and overmatch. Part of the described transformation must include training that helps warfighters to visualize what it means to simultaneously maneuver in all domains with these emerging technologies in a synchronized manner.

For instance, in competition and conflict, U.S. Army forces will experience continuous disruption of command and control (C2) from the EMS, space, and cyber domains. Failure to address these disruptions across domains will cause friendly forces to become isolated without C2 and face a greater risk of defeat during crisis and conflict (McConville, 2021). For these reasons, the U.S. Army introduced its CEMA initiative to provide tactical commanders with integrated cyberspace operations, Department of Defense Information Network (DoDIN) operations, Electromagnetic Attack (EA), Electromagnetic Protection (EP), Electromagnetic Warfare Support (ES), Spectrum Management Operations (SMO), Intelligence, and Information Operations (IO) support/effects. What does this look like for commanders and staff, and how might it be simulated on networks that warfighters train on?

CHALLENGES

Cyberspace is a human-constructed domain consisting of links and nodes that support a multitude of technologies that

are critical to moving data across the other physical domains as units communicate, coordinate, and maneuver in MDO. The challenge is that cyberspace is now more contested and congested that ever, threatening the U.S. Army's ability to maneuver in cyberspace. Moreover, as highlighted in the 2023 National Cybersecurity Strategy, "next-generation interconnectivity is collapsing the boundary between the digital and physical worlds and exposing some of our most essential systems to disruption" (The White House, 2023, p2).

Unfortunately, the understanding, situational awareness, and skills needed for tactical commanders to employ cross-domain capabilities are lacking. Little has been written about tactical cyberspace operations (Schulze 2020), and cyber threats are frequently, if not completely, omitted in scenarios found in virtual training simulations, like Virtual Battle Space (Pyke et al., 2023). Leaders lack resources to guide their use of CEMA with MDO during training exercises and M&S events. As mentioned earlier, even the recent release of TP 525-3-1 fails to mention CEMA, choosing to focus on IEO instead.

The expanding role of CEMA and its merger with IEO ultimately means that doctrine for unit commanders and staff is in flux. Meanwhile, near-peer and peer adversaries have gained ground on the Joint Force's qualitative and quantitative advantages in cyberspace (McConville, 2021). As a result, now more than ever, leaders need to understand how to leverage cyber, EW, and IO capabilities in MDO. More importantly, U.S. Army commanders need to understand how to operate as part of a joint force to fight across all domains and defeat adversaries. In this regard, the CEMA MDO Playbook serves to fill an immediate gap in doctrine and training.

CEMA MDO PLAYBOOK

The CEMA MDO Playbook is tightly coupled with the U.S. Army's current warfighting functions, such as C2, movement and maneuver, fires, and protection. It maps out the operational steps required to conduct actions with available mission systems. Examples of possible scenarios are then tied to these missions that can help Mission Training Centers (MTCs) at Army installations to re-create the effects on these systems to provide an enhanced environment for training or experimentation. Likewise, the Playbook can feed into the creation of a complex, simulated environment that better replicates a realistic, future battlefield.

Motivation

U.S. Army leaders have historically applied a combined-arms approach to create and exploit relative advantages from the land, air, and maritime domains (FM 3-12). However, the proliferation of space and cyberspace capabilities requires leaders to now understand how these capabilities impact their operational environment and their networks if they are to continue creating advantages to exploit in the contested environment that will exist on future battlefields.

Realizing the tactical, operational, and strategic significance of cyberspace operations, the U.S. established the Army Cyber branch in 2014; Electromagnetic Warfare joined the branch in 2018. This convergence brought about numerous opportunities and challenges to warfighters involving doctrine, training, and capabilities. Subject matter experts from government, industry, and academia saw this convergence as an initial step towards a greater goal of controlling information on the battlefield (Cox et al., 2019). However, they also noted that convergence was incomplete with leaders from Division through Brigade struggling to conceptualize what tasks can and cannot be accomplished through EW and cyberspace operations. Similarly, a lack of cyberspace situational awareness was identified as the number one gap in the Army's Cyber/ Electromagnetic (C/EM) Contest Capabilities Based Assessment in 2010 (CAC, 2010). Thirteen years later, this gap remains unresolved in U.S. Army capabilities.

Warfighters have a training and understanding need for how to handle cross-domain intelligence, align it with cyber and EW capabilities, and integrate it all with their warfighting functions. Leaders also struggle to consider the implications of technology to their current mission. For instance, warfighters demonstrate a lack of insight into their equipment's capabilities and vulnerabilities as well as how to best array it to support MDO tasks within the Army and the broader Joint Force. These gaps led the Electronic Warfare Cyber Convergence (EWC2) working group (Cox et al., 2019) to recommend finding or creating mechanisms to tutor senior leaders (Colonel, O6 and above) currently in command and staff positions to fill their individual education gaps in cyberspace operations.

In another recent effort, researchers provided a hypothetical mission description to future Army Officers and challenged them to anticipate up to 25 problems that could arise (Pyke et al., 2023). Despite being "digital natives,"

39% of their research participants failed to anticipate a single cyber threat. This occurred despite the mission description referencing several cyber-vulnerable components (e.g., radios, navigation systems, drones, biosensors, satellites, and cell phones). Digital natives may know how to operate apps and technology but not necessarily how it works or its vulnerabilities. Their research points to the need for warfighters to arm themselves with understanding of their capabilities along with the potential threats that may occur before entering the tactical environment.

The Army's Modeling and Simulation Office (AMSO)—which aims to enable Army processes across acquisition, analysis, experimentation, intelligence, test & evaluation, and training by fostering development of tools, data, and services—is also seeking to address this challenge. AMSO organized a cross organizational functional working group for Cyber & Electromagnetic M&S that has evolved to include developers from space-related organizations to offer a "non-kinetic effects" exchange for professionals to support Army M&S needs and assess emerging capabilities. In February 2023, this group addressed current gaps in M&S technology, tools, data, and services from which AMSO developed focused challenges that it is socializing across the Army through a Council of Colonels (CoC) and a newly re-invigorated General Officer Steering Committee (GOSC). The CEMA MDO Playbook is an example of the type of project that has emanated, at least conceptually, from the cross-organizational collaboration.

Purpose

Current methods for conducting cyberspace operations (including EW) training are incompatible with the traditional, simulation-based training architectures used to conduct battle staff training (Wells, D., 2015), which focused on kinetic events and effects. As a result, there is little consideration of synchronizing the cyberspace domain and the traditional warfighting domains during training exercises.

The Playbook serves to narrow these gaps not only in cyberspace operations but also in EW and information advantage as these elements continue to converge in MDO. Its purpose is to inform tactical (Division and below) commanders–those in "CEMA-for-Others" positions–of their CEMA assets, capabilities, and authorities, as well as those of the organizations that support them. For instance, the Multi-Domain Task Force (MDTF) operates across all domains, providing long-range precision fires, electromagnetic warfare, space, cyber, and information operations, but only the 11th Cyberspace Warfare Battalion[2] has the authority to conduct Offensive Cyberspace Operations (OCO). The Playbook also provides an integrated mapping of impacts/actions/activities on the multi-domain battlefield. Hence, the Playbook helps improve the warfighter's awareness of these capabilities and threats.

Expected conflict scenarios likely to occur during MDO will require high-speed maneuver and rapid decision-making in a contested communications environment marked by degraded information, intelligence, logistics, and mobility (Soesanto, 2021). In simulated scenarios, sensing, understanding, deciding, and acting faster than the adversary will prove crucial to advancing Army objectives and winning. Commanders must know what options exist to manipulate and degrade the threat force's information capabilities to confuse or control adversarial assets. They must also have the opportunity to practice on alternative communications pathways to ensure situational awareness and decision dominance over the adversary. The Playbook provides an initial blueprint for employing CEMA capabilities in MDO, and according to Army Lieutenant Colonel Matthew David, the former commander of the 915th Cyber Warfare Battalion, "Once you have the blueprint, the blueprint lets you build capacity" (Portela, 2021).

Benefits

U.S. Army doctrine offers little on how military planners should envision CEMA tactics and actions working in combination with kinetic operations. Leaders realize they have a dependence on cyberspace and need to fully integrate CEMA within MDO; however, they cannot simulate these converged activities in their home station training environments. Moreover, convergence in MDO includes the rapid and continuous integration of capabilities in all domains, the EMS, and the information environment to achieve cross-domain synergy, mission command and disciplined initiative. With this convergence, warfighters can achieve multiple forms of attack, optimizes effects, and overmatch the enemy. We anticipate this convergence creating three benefits, provided in TP 525-3-1, over single-domain alternatives.

First, leaders will learn through various plays how cross-domain synergy leads to overmatch over adversaries. As

[2] Previously the 915th Cyberspace Warfare Battalion.

leaders examine how various scenarios unfold, they will gain greater confidence in CEMA as a mission enabler and understand how they will impact their operations. The second advantage is familiarization with multiple forms of attack that create layers of options across domains to enhance friendly operations and impose complexity on the enemy. When properly integrated and synchronized as part of a combined arms approach, FM 3-12 states that "cyberspace and EW capabilities can produce layered dilemmas for the adversary in multiple domains and enhance relative combat power" (p. 1-4). Lastly, the Playbook will demonstrate what defensive actions commanders must undertake to protect their network and operations from attacks in the EMS and within the information environment. The Playbook will also assist in translating these actions into simulated events for training and testing.

One advantage that U.S. Forces have in cyberspace operations and EW is that soldiers continually prove resourceful, and they are capable of innovating in the field. Innovation can also be encouraged with more robust training and testing facilities (ADP 3-0). Such options will allow commanders to grow more comfortable quickly introducing changes to plans while executing courses of action (COA) to address a threat force's capabilities and actions in a dynamic, information-rich environment. Likewise, since Cyberspace and EW effects crossover and impact multiple domains simultaneously, leaders can learn to better collaborate across all warfighting functions in MDO – better orchestrating capabilities for higher commands.

CEMA MDO PLAYBOOK

The CEMA MDO Playbook's Playlist consists of a combination of high-level mission threads and more granular plays centered around a specific objective. For instance, some plays are too granular to capture in a common operating picture, yet they are no less important to consider during MDO. Likewise, MDO requires participants to simultaneously engage in offensive and defensive actions in a never-ending game of "cat and mouse." To address these challenges, the Playbook offers graphics that depict a contest of defensive and offensive plays through the lens of CEMA to achieve dominance in MDO. From the CEMA MDO Playbook, we first highlight three depictions: EMS Footprint, Information Operations (IO): Media, and Key Terrain. Other plays considered in the Playbook include Networks, UAVs, and Systems. Following these granular plays, we conclude this section with an example of a mission thread that includes an analysis of cyber, EW, and IO capabilities that could be employed and a short description for requesting and reporting formats that would accompany a training or simulation event.

EMS Footprint

In recent years, the EMS Footprint has taken prominence in detecting and concealing one's location from adversaries. The assumption is that threat forces are always detecting, identifying, locating, and targeting. Figure 1 depicts the defensive and offensive plays that opposing forces might employ.

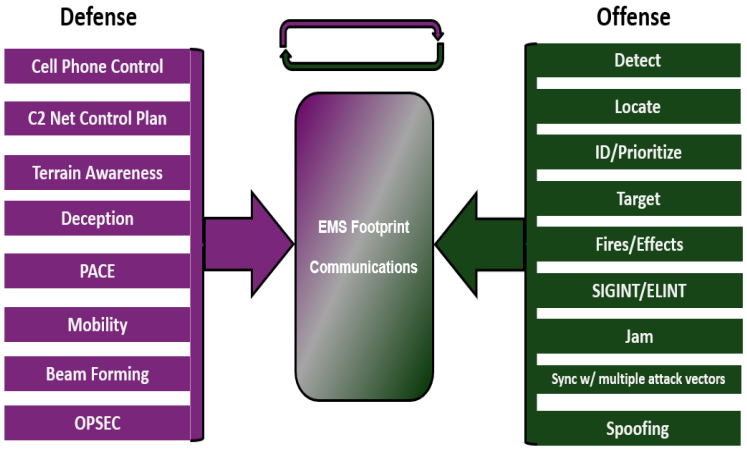

Figure 1. Example of Granular EMS Footprint Plays

As demonstrated in the Ukraine-Russia conflict, personal cell phones have proven an excellent way to identify and target troops in the field. Controlling cell phone usage as well as exercising emitter discipline is critical to avoid targeting by adversaries. Likewise, identifying and targeting adversaries is crucial to mission success.

Other plays in this example consider Primary, Alternate, Contingency, Emergency (PACE) communications along with directional communication methods to avoid an opponent's targeting efforts.

Information Operations (IO): Media

The CEMA MDO Playbook addresses IO: Media from Defensive and Offensive perspectives as shown in Figure 2. One of the most high-profile breaches in recent history occurred in March 2023 when sensitive information regarding the war in Ukraine, as well as on China and US allies–ones briefed at the highest security levels of the Pentagon–surfaced on social media feeds like Twitter, 4chan, Telegram, and the Discord Server that hosts Minecraft (Debusmann, 2023).

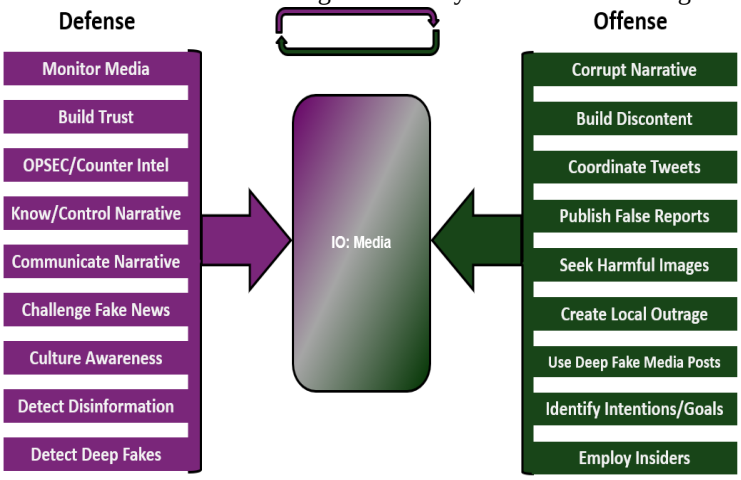

Figure 2. Example of Granular IO:Media Plays

These documents were also manipulated to show numbers that reflect poorly on Ukraine. These efforts indicated a possible disinformation operation by Russia to further stir the chaos caused by the leak. The result was Ukraine had to alter its military plans. Operational security (OPSEC) and counterintelligence efforts were key failures in defense.

Once leaked, offensive actions included identifying intentions and goals and corrupting the narrative to feed disinformation. In contrast, defensive responses include monitoring media sources, detecting disinformation, and challenging fake news or disinformation. These types of circumstances require political and military leaders to quickly get ahead of developing events before misinformation creates conditions on the ground that cannot easily be reversed. Thus, senior leaders must consider IO as part of MDO at all levels.

Key Terrain

Another element critical to mission success in MDO is identifying key terrain in Cyber[3] or mission critical assets and how they might be compromised to understand the risk they pose to the warfighter's mission. Identifying this key terrain and identifying its risks is critical to prioritizing and performing mitigations. See Figure 3.

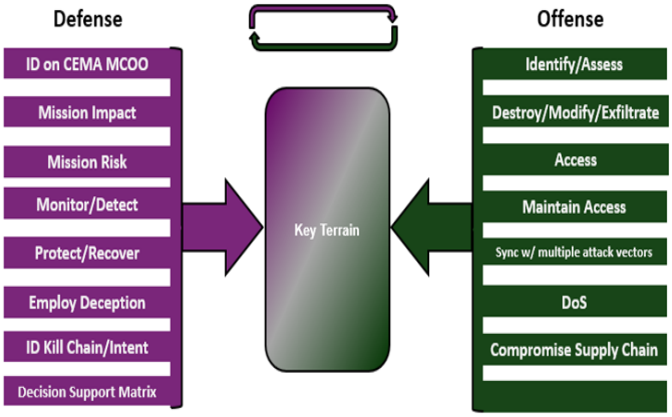

Figure 3. Example of Granular Key Terrain Plays

One reason warfighters must identify and protect their key terrain in cyberspace is most military computing systems rely on distrusted components (Brickey et al., 2012). Over a decade ago, these researchers voiced concerns that many computing systems in the United States rest on a precarious foundation. They noted the U.S. possesses an extremely limited capacity to manufacture advanced microchips, yet rigorous validation of foreign-manufactured circuitry is mostly impossible.

These limitations create opportunities for adversaries to compromise a system from nearly anywhere along the supply chain. Insiders, those trusted to service these systems, represent yet another attack vector, and as wireless capabilities expand, the attack surface of mission systems does as well. Warfighters must identify the assets critical to their mission and wargame how they will monitor, protect, and recover these systems to mitigate the risk of having their mission impacted.

[3] Key terrain in cyber carries numerous connotations. For the purpose of this paper, we use it synonymously with mission critical assets to indicate those mission systems that are critical to a given mission as s given time.

Mission Threads

In accordance with FM 3-12, during MDO, commanders act to dominate the EMS and shape the operational environment. They do so by detecting, intercepting, analyzing, identifying, locating, and affecting (e.g., deny, degrade, disrupt, deceive, destroy, and manipulate) adversary electromagnetic systems that support military operations. At the same time, they work to protect and enable U.S. and Allied Forces' freedom of action in and through the EMS. Mission threads within the CEMA MDO Playbook account for this threat environment where there is an imminent threat of cyber reconnaissance, electromagnetic attack (EA), intelligence surveillance and reconnaissance (ISR), spoofing/jamming, and other threat capabilities to replicate the Denied, Disrupted, Intermittent, and Limited (DDIL) environment expected when in conflict with near- and peer-adversaries.

These challenges must be captured in training and simulation. Plays in the CEMA MDO Playbook are developed within mission threads, so they can readily be adapted into the CEMA M&S Framework (CMFW) (Rob, et al., 2021), which provides a Models Based Systems Engineering (MBSE) approach to systematically survey the breadth of CEMA M&S (Vey, et al., 2019). In the Playbook, mission threads are depicted as CEMA-focused graphics that mimic what a tactical commander and staff might see on their Common Operating Picture (COP). See Figure 4, which provides a condensed view of one mission thread offered in the Playbook where a Brigade Combat Team (BCT) seeks to lure an adversary into giving away their position by implementing a deception in the EMS.

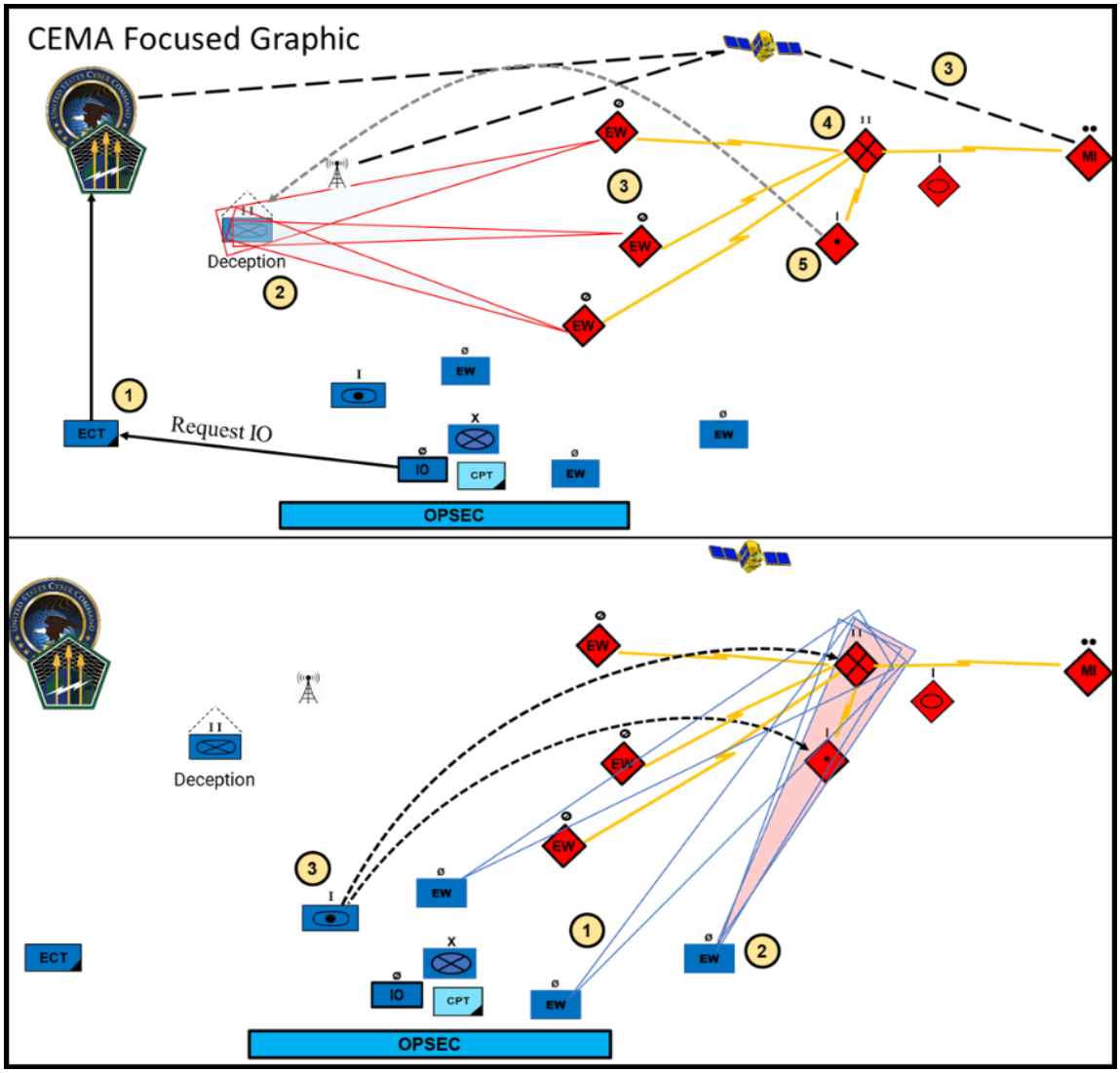

Figure 4. Example of CEMA Focused Graphic Depicting a Mission Thread

This thread is used to demonstrate how CEMA can enable Deception Operations to deceive a near peer threat using deception in the EMS and IO. These signatures might include fake tactical operations centers (TOCs), consisting of false emitters generating pre-recorded wave files that are transmitted via various waveforms and frequencies, while the IO component might consist of social media posts and input into other venues for open-source intelligence.

The deception phase of this mission thread is captured in five steps:

1. The unit begins by requesting IO support through its Expeditionary CEMA Team (ECT) with the intent causing adversaries to believe friendly forces are positioned in a specific location.
2. The commander deploys electromagnetic support (ES) elements to employ deception techniques in the EMS. The result serves to obfuscate the unit's true location while enticing the adversary fire at the decoy and confirm their location. Other ES elements are positioned to scan the operational environment for emissions, while the entire unit exercises operational security (OPSEC) to further obfuscate their location.
3. The adversary soon becomes aware of the decoys location through the IO campaign instigated by the ECT's request to U.S. Army Cyber Command. Scanners also detect the decoy signals.
4. The discovery of the fake unit's location results in multiple radio emissions to inform command and control (C2) elements of the target and to coordinate fires.
5. The fires element delivers effects to the decoy.

The targeting and attack phase is depicted in the lower half of Figure 4.

1. Blue (friendly) forces detect, identify, locate, and target Red (adversary) C2 and Fires locations during the communication stage (step 4 of the top half of the image) and confirms when the adversary fires on the decoy.
2. Blue forces jam the adversary's C2 and Fires elements to intensify the fog of war by sowing confusion within C2 networks and maximize effects on the target.
3. Blue forces deliver effects through fires.

Mission Support

Since it is doubtful that echelons below corps will execute their own cyberspace operations, the Playbook informs commanders and staff of CEMA elements they may request and incorporate into their planning. We previously saw this demonstrated in the above mission thread where the BCT requested IO support through its assigned Expeditionary CEMA Team, which requested support through ARCYBER and U.S. Cyber Command.

While timelines for requesting support are not yet defined in the Playbook, the successful incorporation of cyberspace planning for the brigade combat team should start 180 days before the unit's deployment/rotation (Stover, 2018). However, commanders and staff are introduced to the process of requesting effects beginning with the Cyber Electromagnetics Effects Request Form (CERF) that must be submitted to receive support from Expeditionary CEMA Teams (ECT). As depicted in Figure 4, these teams provide scalability and reach back support for forward units.

In addition to the CERF, the CEMA MDO Playbook also incorporates the Joint Spectrum Interference Resolution (JSIR) Report; the Joint Tactical Air Strike Request (JTASR); the Electromagnetic Attack Request Format (EARF); Electromagnetic Warfare Tasking Message (EWTM); Air Tasking Order (ATO), Annex C, Appendix 12 and Annex H, Appendixes 1, 5, and 6 of the Operation Order; and other requesting and reporting formats essential to training and realistic simulation. Using the Playbook, trainers can ensure warfighters are equipped with the information they need to request resources while M&S developers can incorporate the required formats to support realistic requests.

Playbook Capabilities

Training scenarios and M&S events need to represent cyber and EW capabilities, and a list of capabilities explored in the Playbook are provided in Table 1. Note that the table is primarily focused on cyber, EW, and IO and that delivery of capabilities are left out since their effects can be achieved through multiple attack vectors while warfighters primarily care that the effect is achieved. For instance, the delivery of cyber effects may be accomplished through direct connection, through a media device (e.g., USB), download, email, trusted insider, etc. Additionally, some capabilities, such as targeting, could be accomplished through human intelligence, however, while intelligence staff are included in CEMA working groups, this paper remains focused on cyber operations, EW, and IO.

Table 1. Capabilities Covered in the CEMA MDO Playbook

Capability	Advantages	Disadvantage
Jamming (EW)	Disrupt communication, mislead drones, and other artillery fire correction systems	Targetable
Denial of Service (Cyber)	Disrupt satellite communications, power, and Internet through malware to disrupt enemy command and control (C2)	May reach unintended targets with sever public relations backlash; requires substantial coordination and time to implement.
Spoofing (EW)	Create false coordinates to send GPS-enabled systems off course	Targetable. (Euromaidan, 2023)
Deception (EW & IO)	Mislead reconnaissance and strike drones and obfuscate a unit's true location	Adversary may be able to filter false signals
Targeting (Cyber & EW)	Detect, Identify, Locate, Target through correlation of emitters and networked devices to geographic coordinates	Impacted by Terrain, Noise, and Deception Techniques (Schulze, 2020)
Smishing (Cyber & IO)	Fake text messages demoralize threat forces or set conditions for an ambush	Specific target and information required (Schulze, 2020)
Espionage, sabotage, disruption (Cyber)	Targeting of government, electrical, and economic/financial institutions to disrupt supply chains and create local unrest.	Unintentional impact to civil infrastructure, PR disaster in tense foreign missions (Schulze, 2020)
Data Exfiltration (Cyber)	Gaining access to threat forces operational information	Susceptible to patching and anomaly detection. Little access to air gapped systems
Fake News & Propaganda (IO)	Drives narratives to shape public opinion, confuse adversaries, create local discontent, and discourage political leaders	Requires access to social media feeds and resources where disinformation can be effective

Other capabilities that may be included in the CEMA MDO Playbook at a later date include electromagnetic pulse (EMP). This attack can damage or disable electronic devices. However, these systems come with size, energy consumption, and range constraints with potential for self-inflicted damage (Euromadan, 2023).

DISCUSSION AND FUTURE WORK

Cyber operations have a long planning timeline, making them difficult to integrate into the traditional target cycle of conventional forces during tactical operations (Schulze, 2020). Cyber operations are also far more resource-intensive in their planning (Fink, 2014). For instance, a data connection with enough bandwidth to execute cyber-attacks must exist, and once used, cyber exploits may be less effective in future operations. Current exploits are already a patch away from being rendered useless.

Cyber operations are also highly reliant on reliable intelligence to identify targets. Without it, cyber operations become riskier and much harder to implement with collateral damage becoming far more likely. The intelligence collection and network reconnaissance involved is also a time-consuming process–more so against highly secure, air-gapped targets. Because of these challenges and costs, cyber-attacks are generally best used during the opening stages of conflict where they can contribute to confusion and render initial defenses inoperable.

In contrast, EW is best used during conflict in conjunction with maneuver, fires, and other warfighting functions to expand the fog of war and maximize effects on targets. However, EW capabilities can cut both ways if executed incorrectly, and reliable intelligence is also required. Commanders and staff need to understand how to best employ EW capabilities if they are to create dilemmas for adversaries in real time while creating windows of opportunity for the joint forces.

Through use of the Playbook, commanders and staff will learn the importance of reducing their unit's physical signature through dispersion, use of terrain and camouflage, and mitigate their EMS signatures to ensure operational capability and increase survivability. It will also help leaders visualize domain interconnections and build the "muscle memory" needed to plan and then execute synchronized MDO at speed. Finally, it will introduce options that will allow commanders to grow more comfortable introducing audibles at speed while executing courses of action to address the threat force's capabilities and actions in a dynamic, information-rich environment.

Our work with the CEMA MDO Playbook is certainly not all inclusive and will require further development. Other plays still require exploration to assess their value to MDO. In future work, we plan to include a greater focus on EP. For instance, to date, the Playbook has a significant slant towards EA and ES. We will also seek to align the Playbook with developing Cyber Data Exchange Models (Cyber DEM) and EW Data Exchange Models (EW DEM) to hasten its integration into future M&S efforts[4]. Additionally, following the Army's M&S Forum in 2023, the Council of Colonels (CoC) and General Officer Steering Committee (GOSC) acknowledged a need to further invest in a broader MDO Playbook to explore CEMA and other non-kinetic activities for warfighter understanding and M&S developers.

To evaluate the effectiveness of this work, we see potential in incorporating the Problem Anticipation Task (PAT) methodology (Pyke et al., 2023). The PAT methodology was developed to assess a type of cyber awareness relevant to multi-domain battle, i.e., the ability to anticipate both cyber and physical vulnerabilities in a tactical context. However, their initial research focused on future Army Officers and our efforts focus on seasoned officers at the U.S. Army War College. An obvious extension of the PAT methodology is to gauge tactical cyber awareness in other services and stages of training or career development both before and after Playbook training.

CONCLUSION

In this work, we highlight challenges of educating leaders on the use of cyber operations, electronic warfare, and information operations in multi-domain operations. The U.S. Army and the Joint Force realize that future conflicts will occur across all domains, at longer ranges, and at faster speeds. To meet this challenge, we must re-train the force to consider networks on the move, the importance of electromagnetic protection, and the repercussions of having a footprint in the electromagnetic spectrum. Commanders and staff must also recognize and plan for capabilities that can impact our networks and mission systems in a contested and congested environment. Likewise, they must not only understand communications in the TOC but also communications in all the kill chains (Forward observer, to forward direction center, to gun line). The CEMA MDO Playbook serves to inform training for these leaders as well as requirements for modeling and simulation efforts. With it, warfighters can learn to map Blue (friendly) and Red (adversary) objectives in cyberspace to their objectives in other domains to coordinate efforts and create dilemmas for their adversaries while creating windows of opportunity for the joint forces.

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 EW DEM team, led by Dr. Katherine Morse.

REFERENCES

Bates, C., Heidelbaugh, C., Ruth, J., Friest, T., & Riecken, M. (2021). Using Cyberspace Electromagnetic Activities M&S for Multi-Domain Operations Challenges. 2021 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC). https://www.xcdsystem.com/iitsec/proceedings/index.cfm?Year=2021&CID=862&AbID=97043.

[4] DEM development efforts are led by Dr. Katherine Morse (Morse, 2023) and seek to identify and parameterize the entities and events needed to provide validated data exchange requirements for CEMA across and between live and synthetic environments. Alignment with Cyber DEM and EW DEM efforts will ensure our efforts are unified in a way that supports federation integration across multiple simulation interoperability solutions and training events.

Bates, C., Morse, K., Geddes, A., Heidelbaugh, C., & Rob, J. (2021). Complex Multi-Domain Operational Training: Support Through the Application of M&S. NTSA Webinar Series. TrainingSystems.org. https://www.youtube.com/watch?v=23QPIfPjIiM.

Brickey, J., Cox, J., Nelson, J., Conti, G. (2012). The Case for Cyber. Small Wars Journal. https://smallwarsjournal.com/jrnl/art/the-case-for-cyber.

CAC. (2010). Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA). Draft V 0.9. Combined Arms Center (CAC). Capability Development Integration Directorate (CDID)

Cox, J., Bennett, D., Lathrop, S., Walls, C., LaClair, J., Tracy, C., & Esquibel, J. (2019). The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence. The Cyber Defense Review, 4(2), 81–102. https://www.jstor.org/stable/26843894.

Debusmann, B. (2023). Pentagon documents leak a risk to US national security, officials say. BBC News. https://www.bbc.com/news/world-us-canada-65235121.

Department of the Army. (2019). Army Doctrine Publication (ADP) 3-0 Operations. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf. Web accessed June 2023.

Euromaidan Press. 2023. Russia Ups Its Drone Game With "Mosquito Fleets" and Electromagnetic Warfare. https://euromaidanpress.com/2023/05/06/russia-ups-drone-game-with-mosquito-fleets-and-electronic-weapons/.

Fink, K., Jordan, J., & Wells, J. (2014). Considerations for Offensive Cyberspace Operations. Military Review. 4-11.

FM 3-12. (2021). Cyberspace Operations and Electromagnetic Warfare. TRADOC. https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1022713.

Fogarty, S. G., & Sparling, B. N. (2020). Enabling the Army in an Era of Information Warfare. The Cyber Defense Review, 5(2), 17–28. https://www.jstor.org/stable/26923519.

McConville, J., (2021). Army Multi-Domain Transformation: Ready to Win in Competition and Conflict, Chief of Staff Paper #1, Unclassified Version, Headquarters, Department of the Army. https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf.

Morse, K. (2023). EW-DEM SG – Electronic Warfare Data Exchange Model. https://www.sisostds.org/StandardsActivities/StudyGroups/EW-DEMSG.aspx.

Portela, J., (2021). Cyberspace Battalion Continues Growth with Activation of New Company. Defense Visual Information Distribution Service (DVIDS). https://www.dvidshub.net/news/388197/cyberspace-battalion-continues-growth-with-activation-new-company.

Pyke, A., Ness, J., Feltner, D., (2023). What Types of Tactical Vulnerabilities Do Future Officers Most Anticipate: Are Cyber as well as Non-Cyber Threats on their Radar? Cyber Defense Review (CDR). Army Cyber Institute (ACI). https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Spring/Pyke_Ness_Feltner_CDRV8N1-Spring-2023.pdf.

Schulze, M. (2020). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. 12th International Conference on Cyber Conflict. NATO CCDCOE Publications, Tallinn.

Soesanto, S., (2021). Cyber Defense Report: A Digital Army: Synergies on the Battlefield and the Development of Cyber-Electromagnetic Activities (CEMA). Cyber Defense Project (CDP). Center for Security Studies (CSS), ETH Zurich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-eports-2021-08-Creating-Synergies-on-the-Battlefield-CEMA.pdf

Stover, S. (2018). Army developing expeditionary cyber-electromagnetic teams to support tactical commanders. https://www.army.mil/article/200262/army_developing_expeditionary_cyber_electromagnetic_teams_to_support_tactical_commanders.

The White House. (2023). National Cybersecurity Strategy. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

TP 525-3-1. (2018). The U.S. Army in Multi-Domain Operations 2028. TRADOC Pamphlet. https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf.

Turgai, J. (2023). Cyber Warfare Lessons from the Russia-Ukraine Conflict. Dark Reading. https://www.darkreading.com/attacks-breaches/cyber-warfare-lessons-from-russia-ukraine-conflict.

US Strategic Command (USSTRATCOM). (2020). Joint Electromagnetic Spectrum Operations (JP-385). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf

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

Wells, D., & Bryan, D. (2015). Cyber Operational Architecture Training System – Cyber for All. 2015 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC). https://www.iitsec.org/-/media/sites/iitsec/link-attachments/best-papers-and-tutorials-from-past-iitsec/15108_sim_paper.ashx?la=en