CEMA: A Key to Success in Unified Land Operations

MISSION MC COMMAND

The Army has recently codified the concept of cyber-electromagnetic activities (CEMA) within its doctrine. At its heart, CEMA is designed to prepare the Army to address the increasing importance that both cyberspace and the electromagnetic spectrum will play in the success of unified land operations.

According to ADP 3-0 Unified Land Operations, CEMA involves "activities leveraged to seize, retain and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system." It is implemented via synchronization and integration of three lines of effort: cyberspace operations, electronic warfare (EW) and electromagnetic spectrum operations (EMSO).

By BG Wayne W. Grigsby Jr.,
COL J. Garrett Howard,
Tony McNeill
and
LTC Gregg Buehler,
U.S. Army retired

iStockphoto

Longbow radar (in a close up on an Apache attack helicopter) is a millimeter-wave fire control radar that offers exceptional targeting capability. Visible just behind the main rotor assembly, an infrared jammer improves survivability against heat-seeking missiles.

and DoD global information grid operations (build, operate and maintain).

EW is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection and electronic warfare support.

EMSO consists of planning, operating and coordinating the use of the electromagnetic spectrum through operational, engineering, administrative and policy implementation procedures to enable wireless electronic systems to function in the intended environment without causing or suffering unacceptable "frequency fratricide."

When stressed by the commander and integrated by the staff, CEMA can play a critical role in the successful execution of decisive action. Analysis from recent history and emerging trends within the operational environment (OE) support this assertion. The world in which U.S. forces operate is increasingly wireless and computer network-based. Rapidly evolving information technologies are expanding the speed, capacity, agility, efficiency and usefulness of modern networks. The proliferation of these systems is changing the way humans interact with each other and their environment, including military operations. This creates conditions that will make U.S. forces increasingly dependent on these technologies and require soldiers to counter technology-empowered and sophisticated adversaries who can utilize commercial industry and the network as their primary combat developers. This broad and rapidly changing OE will present a plethora of potential threats and opportunities that are primarily limited by our own—and our opponents'—imagination, causing the Army to operate within a cyberspace domain and EMS that are increasingly congested and contested.

In addition, it's important to recognize the convergence of cyber and EMS capabilities. Commercial and military systems are increasingly reliant on both as networks and telecommunication infrastructures expand their use of wireless means. This is particularly important for collaborative systems that require connectivity to operate effectively. The synergistic effect of these networks is a significant reason why EW, EMSO and cyber operations must be viewed as interrelated and interdependent. Though organizations are already executing these tasks to some degree throughout the Army, the inherent interrelationship among these three components demands that they be closely synchronized to optimize

Cyberspace operations employ capabilities to achieve objectives in or through cyberspace. The three main components of cyberspace operations are offensive cyber operations (attack, exploit), defensive cyber operations (defend)

BG Wayne W. Grigsby Jr. *is the director of the Mission Command Center of Excellence at Fort Leavenworth, Kan. Previous assignments include director of the School for Advanced Military Studies; chief of International Security Assistance Force Joint Command's Future Operations Cross-Functional Team during the Afghanistan surge; and commander of the 3rd Brigade Combat Team, 3rd Infantry Division, during the Iraq surge.* ***COL J. Garrett Howard*** *is director of the U.S. Army Electronic Warfare Proponent Office at Fort Leavenworth. Prior assignments include chief intelligence planner in Iraq on the Multi-National Force-Iraq staff. He has commanded military intelligence units at the company, detachment and battalion levels.* ***Tony McNeill*** *is deputy director of the Electronic Warfare Proponent Office at Fort Leavenworth. He is the lead author of Field Manual (FM) 3-36* Electronic Warfare in Operations*. A former Marine Corps lieutenant colonel, he last served as deputy director and chief instructor within the Marine Corps Element at the Army Command and General Staff College.* ***LTC Gregg Buehler****, USA Ret., is doctrine and organizations section chief within the Electronic Warfare Proponent Office at Fort Leavenworth. He is the lead author of FM 3-38* Cyber-Electromagnetic Operations *and recently completed the revision of FM 3-36. Previously he served as the chief of organizations development within the Proponent Office and the lead for the Force Design Update for Electronic Warfare.*

iStockphoto

their potential impact on the execution of decisive action.

Informed by these observations, the Army built the CEMA construct on several important assessments. Commanders play a central and critical role in CEMA: They must ensure that cyberspace and the EMS are viewed as important elements within their analysis of the OE, and they must recognize that it is possible to gain an operational advantage over an adversary within these areas and that such an advantage can be decisive in the conduct of operations. This can occur at all levels of warfare (tactical, operational and strategic) and organizational echelons. Conversely, to allow an adversary to gain such an advantage or to lose the freedom of movement within cyberspace and the EMS will set one at a significant disadvantage.

In turn, this will require commanders to reexamine their view of what constitutes combined arms. This does not mean that one forgoes or diminishes the importance of traditional weapons systems (lethality still matters) but instead that one recognizes that commanders should consider cyber, EW and EMSO capabilities as part of the combined arms construct as the equal of their more traditional counterparts. Implicit in this point is that commanders must be able to address cyber, EW and EMSO via the same operations process and integrating functions as any other available resource.

The requirement for full integration of these capabilities, the dependency of mission command systems on the EMS and cyberspace, and the commander's critical role in using these capabilities resulted in the Army's decision to conduct cyber-electromagnetic activities within the mission command warfighting function.

To fully empower commanders with the tools they need to execute decisive action, the Army is aggressively pursuing ways to bring more cyber, EW and EMSO capabilities down to the tactical edge. Given the recent embrace of the CEMA construct, this also includes seeking ways to provide commanders (brigade combat team and above) with an organic means to integrate these activities into the operations process.

To some degree, this integration is already occurring. Soon-to-be-published revisions to Field Manual 3-36 *Electronic Warfare in Operations* will task the commander's EW element to expand and use the EW working group to facilitate CEMA integration. This is intended only as a bridge, however, until the Army develops a more appropriate means to achieve this. Army Cyber Command and the Mission Command Center of Excellence are co-leads in the Army's effort to determine how best to accomplish CEMA integration for the long term.

Current plans envision CEMA integrated within the operations process via the Cyber-Electromagnetic Working Group (CEMWG) and integration efforts led by a cyber-electromagnetic (CEM) staff element. The role of the CEMWG will be to integrate and synchronize cyberspace operations, EW and EMSO to maintain freedom of action while denying our adversaries the same, ultimately to achieve the commander's intent and operational objectives.

The CEMA element, the composition of which is to be determined, will focus on two important functions. First, it will seek to integrate and synchronize cyber-electromagnetic capabilities and activities to achieve desired conditions in the cyberspace domain and across the EMS. This will involve unifying the offensive and defensive aspects of cyber-electromagnetic activities and orienting them on the commander's stated objectives. To this end, the CEM element serves as the source of cyber-electromagnetic situational awareness and continually assesses progress toward desired conditions. The CEMA element integrates all appropriate capabilities to achieve these desired ends. Second, the element will integrate cyber-electromagnetic activities as part of combined arms.

Both functions will be accomplished within the staff's three integrating cells: current operations, future operations and plans. The CEM element will coordinate the critical components of cyber-electromagnetic activities across all the warfighting functions and staff elements (G/S-2, G/S-3, G/S-6, and so on) both vertically and horizontally. This includes integration with external staffs, organizations and coalition partners. Given the very dynamic nature of cyber-electromagnetic activities, the CEM element will likely require a presence in the current operations cell and may need colocated representatives from the G/S-2, G/S-3 and G/S-6 (and potentially others) to achieve real-time awareness, direct dynamic actions and responses to unfolding conditions.

Determining how to address the challenges and opportunities that cyberspace and the EMS present our forces will remain an evolving process. Time, technology, available resources and a plethora of other factors will influence how the Army develops its solutions. What is certain is that the need to operate within this part of the commander's OE will remain and that to gain and maintain an advantage in cyberspace and the EMS will be vital to successful unified land operations. ★