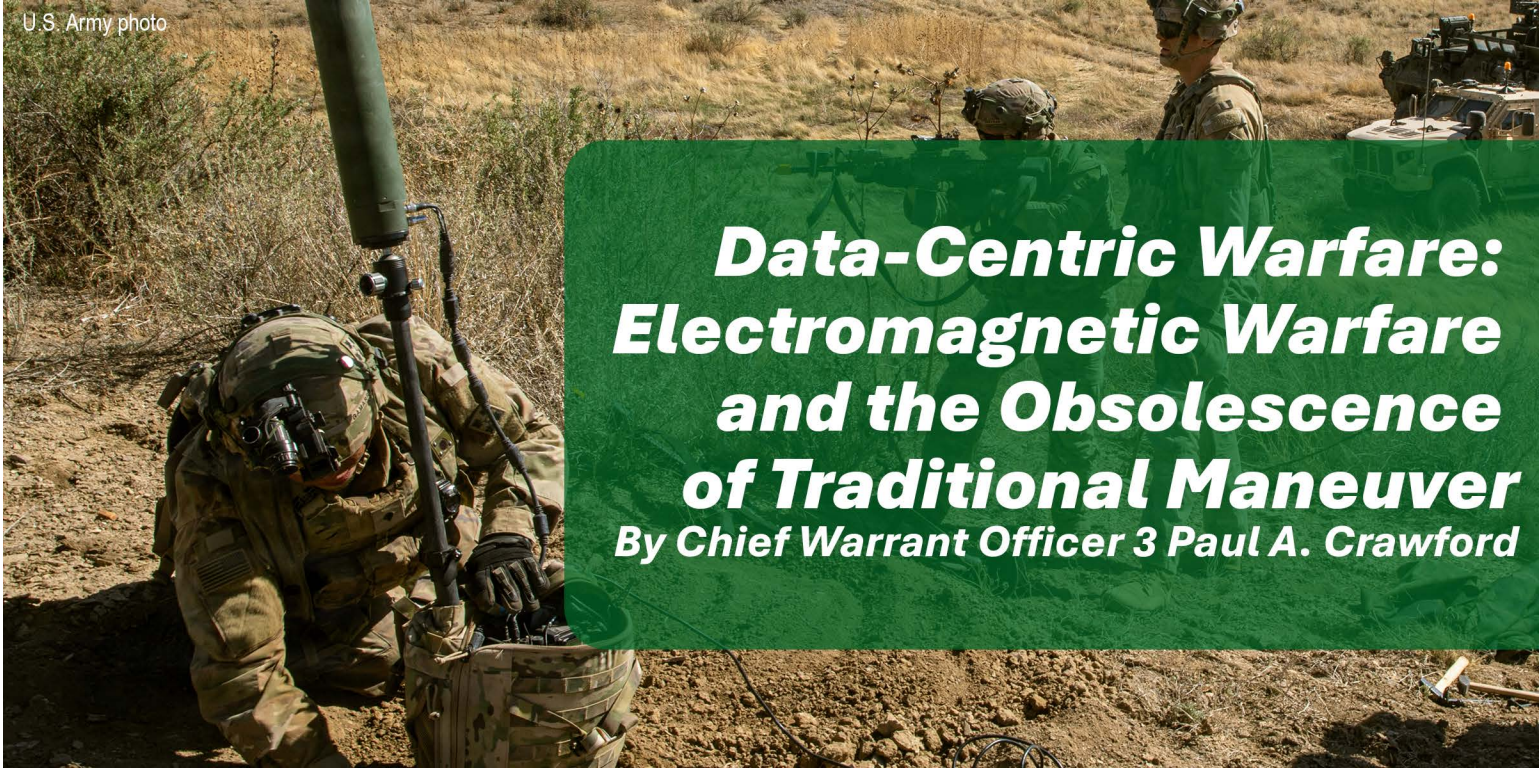

U.S. Army photo

Data-Centric Warfare: Electromagnetic Warfare and the Obsolescence of Traditional Maneuver

By Chief Warrant Officer 3 Paul A. Crawford

The Electromagnetic Blind Spot

On a future battlefield, a division G-2 prepares the section to support a wet gap crossing. Thus far, the operation has proceeded according to plan. Subordinate brigades advance uncontested to secure their attack positions, and the reconnaissance and security brigade (RSB) pushes forward to secure the far side objective. The division strike cell has identified high-payoff targets and passed the coordinates to the division artillery.

Yet, the guns remain silent. Risk mounts rapidly for the scouts, who are now in direct contact.

A heavy silence settles over the current operations integration center. The G-2 suspects an electromagnetic attack is underway but hesitates to speak—electromagnetic warfare was omitted from the planning process. When the commanding general demands an update, the staff cannot provide a frontline trace or an accurate enemy situation map.

While the commander and staff deliberate, enemy rockets and attack aviation devastate the RSB. Precision artillery fire begins to systematically degrade the bridging company and brigade command posts. The division's entire intelligence and command and control architecture disintegrate under a barrage of physical and electromagnetic fires. Within 60 minutes, the wet gap crossing has failed, and half the division's combat power is gone.

Introduction

The characters of war has fundamentally changed. Army Field Manual 3-0, *Operations*, observes that warfare "may retain similarities over time, but it inevitably also has great variations."[1] Today, the era of traditional wet gap crossing and deliberate breach operations as primary tactical solutions has passed. This evolution stems from tactical observations of the Russo-Ukrainian War and, more importantly, the rapid maturation of emerging technologies: artificial intelligence-enabled decision making, deep sensing, long-range precision fires, autonomous systems and space-enabled capabilities.

Because these advanced systems rely entirely on uninterrupted data streams, military doctrine must adapt to a new paradigm: data-centric warfare.

In data-centric warfare, data control dictates technological mastery. The complexity of synchronizing and integrating these capabilities will accelerate the tempo of operations, driving new tactics to achieve decision dominance, unrivaled sensor-to-shooter speed, and shorter, more destructive conflicts. Because modern military capabilities are only as effective as the links that connect them, the center of gravity in data-centric warfare is access to and control of the electromagnetic spectrum (EMS). The U.S. Army must therefore rethink maneuver, adopting systemic disintegration as its primary defeat mechanism to achieve EMS superiority.

Historical Context

The last time the U.S. Army fundamentally rethought maneuver was in the wake of World War I, a conflict fought with 18th-century tactics using 20th-century equipment. While air power, machine guns, massed artillery, and early armor should have accelerated the tempo of war, antiquated tactics and a technology-doctrine mismatch instead yielded the stagnation of trench warfare. Entire formations charged across "no-man's-land" into defensive fires, suffering catastrophic casualties for negligible gains.[2]

Following the war, Germany developed a mechanized military built around Blitzkrieg ("lightning war"). This doctrine harmonized technological advancement in radio communication, armor, and close air support to bypass and isolate enemy strongpoints. In 1939, this mobile, combined-arms approach allowed Germany to rapidly overpower European militaries that lacked the doctrine or mechanization to counter it. It took years for the Allied powers to develop comparable

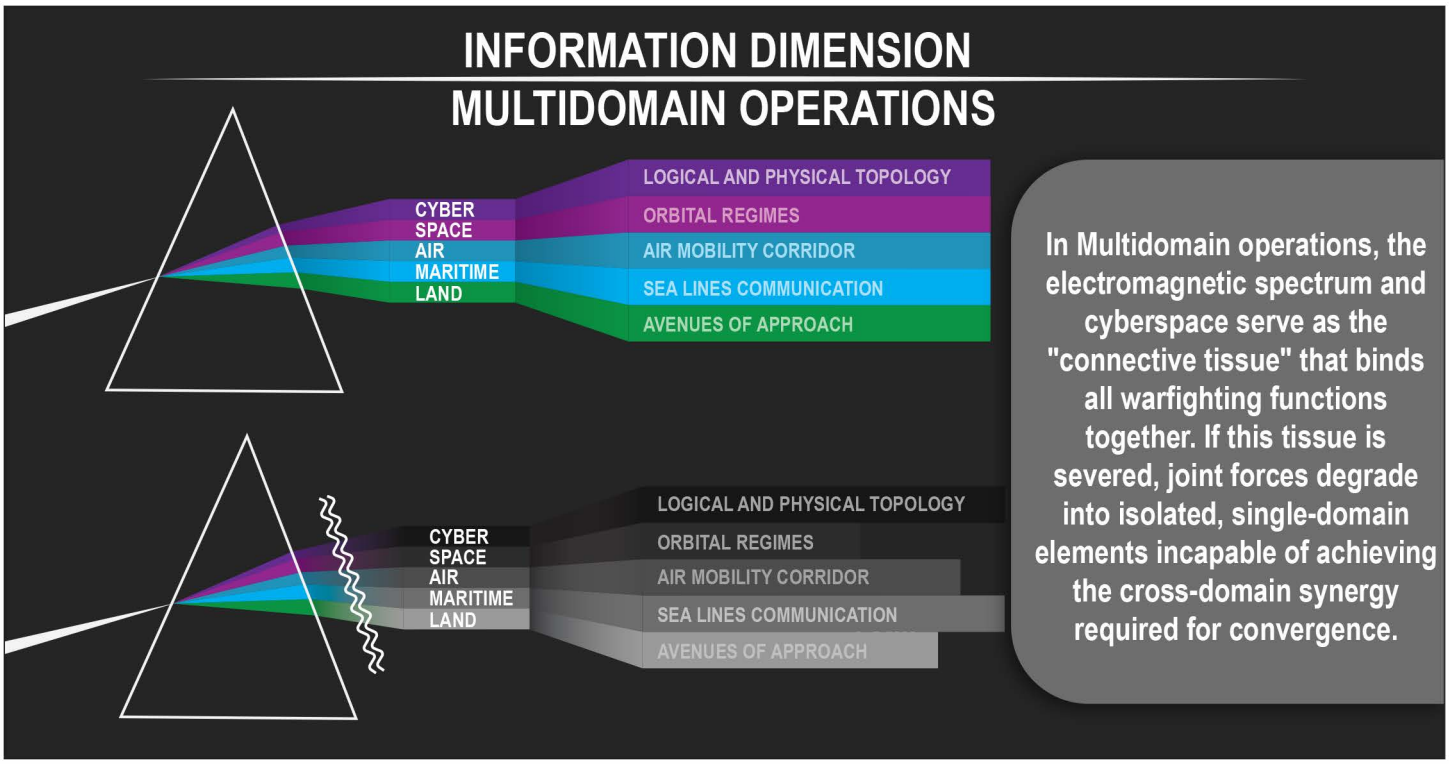

Figure. Multidomain Maneuver

technologies and tactics. Ultimately, the Allies prevailed, aided by Germany's strategic overextension and its failure to develop a nuclear capability before the United States.[3]

Today, the joint force stands at a similar crossroads, and technological advancements are outpacing doctrine. Successfully synchronizing and integrating multidomain capabilities highlights the steep requirements of this new, data-driven era.

The New Key Terrain

Data-centric warfare depends on the seamless interconnection of multiple systems to synchronize sensors and shooters across land, sea, air, space, and cyberspace. Consequently, EMS superiority is the ultimate high ground. Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations*, defines EMS superiority as "that degree of control in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting the threat's ability to do the same."[4] To force the culmination of adversary operations, friendly forces must execute systemic disintegration to isolate and disable key enemy capabilities.

Achieving EMS superiority requires electromagnetic warfare (EW), which comprises three functional areas: electromagnetic support (ES), electromagnetic attack (EA), and electromagnetic protection (EP). By effectively employing these capabilities, friendly forces can protect their own links while disrupting, degrading, or destroying those of the enemy.

- **Electromagnetic Support:** ES serves two critical functions: reconnaissance and command and control (C2). In its reconnaissance role, ES identifies and characterizes enemy signals for future engagement and provides battle damage assessment of EA effects. In its C2 role, ES task-organizes EW assets into tactical formations—such as fires, air defense, maneuver, or logistics—and synchronizes spectrum operations with maneuver.[5]
- **Electromagnetic Attack:** EA is the offensive use of electromagnetic energy to disrupt, degrade, or destroy enemy systems. By jamming satellite or radio communications, EA prevents an adversary from massing forces and isolates geographically dispersed units.[6]
- **Electromagnetic Protection:** EP is the defensive component of EW. Examples include fiber-optic connections, frequency hopping, spectrum management, emission control, and hardware hardening. These preventive countermeasures protect friendly data links and ensure operational freedom of maneuver.[7]

Electromagnetic Warfare Employment

Once EW severs an adversary's data links, traditional maneuver forces can engage and destroy the resulting isolated pockets of capability. Deprived of communication, adversary maneuver units lose situational awareness, C2 nodes cannot synchronize operations, logistics chains stall, intelligence, surveillance, and reconnaissance assets go blind, and fires units are unable to execute missions. Friendly forces can then destroy these isolated elements in sequence.

The challenge lies in severing the adversary's communication networks while protecting our own from similar disintegration. Friendly forces can achieve this through two primary methods:

Layered Redundancy. Layered redundancy combines robust communication access with disciplined spectrum management to deny the adversary the ability to systematically disintegrate friendly forces.

- **PACE Planning:** Friendly forces must establish a primary, alternate, contingency, and emergency (PACE) communications plan. This plan should combine space-based, high-altitude, and ground-to-ground radio systems with physical fiber-optic networks. The variety and depth of access force the adversary to expend diverse ES and EA assets, making complete denial highly difficult.
- **Spectrum Management:** This involves emission control and electromagnetic masking. Emission control restricts transmissions to predetermined windows to minimize detection. Electromagnetic masking conceals signatures by generating decoy signals or distributing electromagnetic profiles, preventing the adversary from geolocating key command nodes.

Key EW Capabilities Targeting. The second method directly targets adversary EW capabilities at every echelon. To deny or disrupt these critical networks, the joint force must penetrate enemy defenses. Because the adversary deploys EW assets throughout their formation, including static, hardened infrastructure, targeting is highly complex.

However, by remaining concealed within the EMS and simultaneously isolating the enemy's EW C2 nodes, U.S. forces can neutralize the adversary's ability to employ these systems. This approach demands precise joint synchronization to identify and target specific electromagnetic signatures. For example, denying an adversary's ground jamming requires understanding not only the variety of jamming assets, but also their specific C2, power, manning, communications, and electronic support profiles. Ultimately, failure to neutralize these adversary EW capabilities imperils all follow-on military operations.

Conclusion

To survive and win on the modern battlefield, friendly forces must dominate the EMS during the critical phases of an operation. We must execute maneuvers with unprecedented speed and surprise, drastically reducing the window of time our communication networks are exposed. This compressed timeline deprives the adversary of the window they need to target us, while enabling friendly forces to rapidly concentrate combat power at the decisive point.

Mastering spectrum concealment and neutralizing enemy deep-sensing software strips away the adversary's technology-driven advantages. By forcing the enemy to rely on human talent and decentralization rather than automated systems, the U.S. Army shifts the conflict into a chaotic, fast-paced arena that rewards tactical proficiency, initiative, and decentralized leadership—areas where the American warfighter holds an overwhelming advantage.

Endnotes

1. Headquarters (HQ) Department of the Army, Field Manual 3-0, *Operations* (Government Publishing Office [GPO], 2025), 8.

2. Timothy T. Lupfer, *The Dynamics of Doctrine: The Changes in German Tactical Doctrine During the First World War* (U.S. Army Command and General Staff College, 1981).

3. Lupfer, *The Dynamics of Doctrine*; and Kristen D. Burton, "The Scientific and Technological Advances of World War II," The National WWII Museum, July 30, 2020, https://www.nationalww2museum.org/war/articles/scientific-and-technological-advances-world-war-ii.

4.Chairman of the Joint Chiefs of Staff, Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations* (Joint Staff, 2026), GL-5.

5. HQ, Department of the Army, Army Techniques Publication 3-12.3, *Electromagnetic Warfare Techniques* (GPO, 2024), 6-1–6-14.

6. Ibid., 4-1–4-17.

7. Ibid., 5-1–5-17.

CW3 Paul Crawford is currently assigned as the Officer in Charge of the Intelligence Reach Operations Center, 4th Infantry Division G-2, where he provides electronic warfare-focused target system analysis support to U.S. Pacific Command. Previously, CW3 Crawford served in the 4th Security Force Assistance Brigade (SFAB), supporting six U.S. Army Europe-Africa and NATO exercises at the division and corps levels. During this tenure, he led multiple military-to-military engagements in Europe to enhance partner and ally intelligence capabilities and deployed as part of the first 4th SFAB brigade-level deployment in support of the Russo-Ukrainian Conflict in 2022. Throughout his career, he has served in the 173rd Infantry Brigade Combat Team (Airborne), 82nd Airborne Division, 7th Special Forces Group (Airborne), 1st Infantry Division, 4th SFAB, 4th Infantry Division. His operational deployments include three combat tours to Afghanistan and one non-combat tour to Poland.