Designating the Electromagnetic Spectrum (EMS) as an Operational Domain

CW2 Jeff B. Newsome and CW2 Travis M. Whitesel

The concept of military domains has traditionally encompassed air, land, maritime, space, and cyberspace, each defined as mediums for maneuver and control to achieve strategic objec-tives (ADP 3-0, 2019; FM 3-0, 2022). With the increasing dependence on and complexity of electromagnetic spectrum (EMS) operations, evaluating whether EMS should also be designated as an independent domain is essential. EMS is classified under cyberspace due to its role in data transmission. However, this oversimplification overlooks the EMS's broader utility and necessity in modern warfare, particularly in electronic warfare (EW) activities—attack, protect, and sup-port—pivotal to battlefield superiority (JP 3-85, 2020).[TW1.1]

Definition of Military Domains

A military domain is a medium an actor must access, maneuver within, and control to achieve its objectives in a conflict. According to joint military doctrine, current domains include air, land, maritime, cyberspace, and space. Conflict in each domain requires unique strategic ap-proaches due to the medium's physical and operational characteristics. For example, operations in the air domain depend on altitude, speed, and air control, while the maritime domain relies on waterborne maneuverability. Similarly, cyberspace operations hinge on data integrity, network connectivity, and access to digital systems, while the space domain requires control over orbital pathways and space-based assets (JP 3-0, 2022b; JP 3-12, 2022a).[TW2.1][TW2.2]

The Electromagnetic Spectrum (EMS): Definition and Strategic Importance

EMS encompasses all frequencies of electromagnetic energy, including radio, microwave, infrared, visible light, ultraviolet, X-rays, and gamma rays. It is the backbone for critical military operations such as communication, radar, jamming, electronic surveillance, and precision target-ing. Control over EMS enables forces to detect, track, and target adversaries, which is crucial for achieving operational dominance in other domains. As a medium, EMS is essential not only for digital communication but also for conducting electronic attacks, defenses, and support opera-tions that influence the broader conflict environment (JP 3-85, 2020).

EMS in Relation to Cyberspace and Other Domains

Military operations increasingly depend on the EMS for data transmission, as a conduit for communications, radar, and weapon guidance systems, and to enhance situational awareness (JP 3-12, 2022a). While cyberspace serves as the operational sphere for information and network security, EMS provides the medium across which these and other critical capabilities operate, ex-tending to electronic attack, support, and protective measures. For example, the Army's opera-tions doctrine describes EMS as an essential component of EW, integral to controlling the opera-tional environment, thus necessitating a dedicated focus beyond cyberspace (FM 3-12, 2021b; AR 525-24, 2023).

Although cyberspace relies on EMS for data transmission, the relationship between the two is not synonymous. Cyberspace focuses on digital networks, data integrity, and virtual inter-actions, while EMS deals with electromagnetic energy across a wide frequency range used for both digital and non-digital

applications. For example, while cyberspace operations might involve securing data on a network, EMS operations could involve jamming an adversary's radar or communications. These functions highlight EMS's broader applications, encompassing digital and physical effects that cyberspace alone cannot achieve. This distinction underscores the need to treat EMS as a separate operational domain rather than a subcategory of cyberspace (FM 3-12, 2021b; JP 3-85, 2020).

Challenges of Integrating EMS into Cyberspace Operations

Integrating EMS under cyberspace demeans its function, limiting military strategy and oversight.[TW3.1] Current doctrine often fails to capture EMS's unique capabilities, such as elec-tronic warfare's ability to disrupt enemy operations without engaging in physical combat. [TW4.1][TW4.2]As a result, it is possible that commanders do not understand its full functionali-ty and request to deploy cyber forces when they mean EW. This can result in delayed operations or confusion for the staff regarding what capability to deploy. When EMS is confined to cyber-space, the strategic focus narrows to network and data security, overlooking critical aspects of electronic warfare. For instance, radar jamming, deception, and directed energy weapons operate within EMS but are not directly aligned with cyberspace's core focus on data and networks. This paper argues that separating EMS would improve clarity and operational focus, allowing forces to develop specialized EMS tactics that maximize its unique characteristics (FM 3-0, 2022; JP 3-0, 2022b).

Cyberspace operations focus on information networks, seeking to secure, exploit, or ma-nipulate data within and across these networks (JP 3-0, 2022b). In contrast, EMS operations en-compass a physical range of frequencies for communication and signal-based operations, which include jamming, spoofing, and sensing. As EMS encompasses a broader range of applications beyond just data movement, it requires a dedicated approach to fully leverage its unique opera-tional properties (Chief of Staff Paper #1, 2021a). Unlike cyberspace, where operations primarily seek data manipulation, EMS operations directly impact the tactical and strategic environment by altering the electromagnetic operational environment (EMOE).

The Role of Electronic Attack, Protect, and Support within EMS

The scope of EMS capabilities—spanning electronic attack (e.g., disrupting enemy radar), electronic protection (e.g., securing communications against jamming), and electronic support (e.g., detecting adversarial signals)—illustrates its distinct contributions to combat operations. In high-stakes environments like the Indo-Pacific, where communication systems face considerable interference risks, establishing EMS as a separate domain would allow more precise strategic alignment and resource allocation (FM 3-0, 2022; JP 3-85, 2020). Additionally, as joint force op-erations grow increasingly complex, designating EMS as a distinct domain would streamline command and control structures, enabling dedicated resources and personnel to optimize the full scope of EMS applications across various conflict levels.

Electronic Attack (EA)

Electronic Attack (EA) involves using the Electromagnetic Spectrum (EMS) to degrade, disrupt, or deny enemy electronic systems, such as radar and communication networks, support-ing tactical and operational objectives. Techniques like jamming or deceiving enemy radar ob-scure friendly force movements, ensuring greater operational security and maneuverability (FM 3-12, 2021b; JP 3-85, 2020).

Electronic Protect (EP)

Electronic Protect (EP) safeguards friendly EMS capabilities from adversarial attempts to disrupt or deny access. This includes implementing defensive measures to secure military com-munications and navigation systems against jamming or interference, thereby maintaining opera-tional effectiveness in contested environments (FM 3-12, 2021b; JP 3-85, 2020).

Electronic Support (ES)

Electronic Support (ES) entails collecting intelligence and situational awareness through EMS activities, such as intercepting enemy signals. These operations enable real-time insights into adversary movements and capabilities, essential for informed decision-making and tactical ad-vantage on the battlefield (FM 3-12, 2021b; JP 3-85, 2020). While EMS operations may comple-ment cyberspace efforts, these functions underscore that EMS operates as an independent do-main critical to achieving strategic dominance in contemporary conflicts.

Benefits of Designating EMS as a Separate Operational Domain

Designating the Electromagnetic Spectrum (EMS) as its own domain would enable the military to fully control and exploit EMS capabilities by separating them from the cyberspace domain. This distinct designation would provide a structured framework for developing special-ized tactics, command and control (C2) enhancements, and strengthened defenses crucial for modern conflict (JP 3-12, 2022a; JP 3-85, 2020).

Development of Specialized Tactics and Training [TW5.1]

Recognizing EMS as an independent domain would allow us to create targeted training programs and develop tactics specifically suited for EMS operations. It would also enable us to train professionals in EMS to counter adversarial use of the domain. This focus would improve operational effectiveness in contested environments where control over EMS is vital for mission success (JP 3-12, 2022a; FM 3-12, 2021b).

Improved Command and Control (C2)

A separate EMS domain would give commanders more explicit oversight and control by defining responsibilities within a dedicated structure. This approach would help prevent overlap or confusion with cyberspace operations, allowing for a more streamlined and effective C2 pro-cess (JP 3-12, 2022a).

Strengthened Defense and Resilience

Given the increasing sophistication of electronic warfare threats, establishing EMS as its own domain would strengthen military defenses against complex threats. Enhanced resilience against attacks on GPS, communication systems, and radar would protect critical assets and en-sure operational continuity (JP 3-12, 2022a; JP 3-85, 2020).

Policy Recommendations and Future Research

Develop EMS-Specific Doctrine

Crafting a doctrine specifically for the Electromagnetic Spectrum (EMS) would address its distinct operational needs independent of cyberspace. This doctrine should outline strategies encompassing electronic attack, protection, and support functions, ensuring that EMS capabilities are fully utilized in various operational scenarios (JP 3-12, 2022a; JP 3-85, 2020).

Enhance International EMS Norms

Establishing global standards for EMS operations, similar to norms in other domains, would mitigate risks of misinterpretation or escalation in multinational contexts. Explicit interna-tional norms would promote responsible EMS usage and help stabilize relations during collabora-tive or contested engagements (JP 3-85, 2020).

Integrate EMS into Multi-Domain Operations (MDO)

Incorporating EMS-specific capabilities into Multi-Domain Operations (MDO) doctrine would enhance joint force effectiveness. EMS plays a critical role across domains, so leveraging it within MDO would enable forces to coordinate and capitalize on EMS's unique advantages during operations (FM 3-12, 2021b). Further research is essential to address the economic, politi-cal, and technological factors associated with formalizing EMS as a separate domain. This re-search should assess the impacts on training requirements, resource distribution, and international collaboration and explore how these factors would shape a dedicated EMS framework (Chief of Staff Paper #1, 2021a).

Conclusions

Designating EMS as its own operational domain recognizes its strategic role beyond the confines of cyberspace, emphasizing its unique capacity to influence the battlefield across the competition continuum. By advancing EMS as a separate domain, the military can optimize elec-tronic warfare capabilities and better secure the electromagnetic environment essential for mod-ern warfare (JP 3-12, 2022a). As technological and operational landscapes evolve, this distinction will ensure EMS resources are effectively integrated and prioritized, providing a solid foundation for future conflict environments.

Author Biography

CW2 Jeff B. Newsome is an active-duty Army Military Intelligence Warrant Officer. Jeff was appointed a Warrant Officer in August of 2019. He graduated from American Military Universi-ty (AMU) with his master's degree in intelligence operations with a concentration in homeland security in December 2022. He is pursuing a Doctorate in Strategic Intelligence (DSI) at AMU. In his previous assignment, he served as a Brigade Fusion Chief for S2, HHC, 2nd SBCT at Fort Carson, CO. He is currently the Regional Cyber Center (RCC) Intelligence Support Element (ISE) Cyber Intel Section Chief for RCC-E, NETCOM, ARCYBER at Fort Huachuca, AZ.

CW2 Travis M. Whitesel is an active-duty Army Cyber Warrant Officer. Travis was appointed a WO in February of 2019. He graduated from American Military University (AMU) with his master's degree in national security studies with a concentration in cyber operations in February 2023. He is pursuing a Doctorate in Cybersecurity at National University. He is currently NET-COM G2's Senior Technical Advisor and serving as Regional Cyber Center (RCC) Intelligence Support Element (ISE) ISE OIC for

RCC-SWA, NETCOM at Fort Huachuca, AZ. He can be contacted at travis.m.whitesel.mil@army.mil.

References

Department of the Army. (2019). Operations (ADP 3-0).

Department of the Army. (2021a). Army multi-domain transformation (Chief of Staff Paper #1).

Department of the Army. (2021b). Cyberspace operations and electromagnetic warfare (FM 3-12).

Department of the Army. (2022). Operations (FM 3-0).

Department of the Army. (2023). U.S. Army cyberspace and electromagnetic warfare operations (AR 525-24).

Joint Chiefs of Staff. (2020). Joint electromagnetic spectrum operations (JP 3-85).

Joint Chiefs of Staff. (2022a). Cyberspace operations (JP 3-12).

Joint Chiefs of Staff. (2022b). Joint campaigns and operations (JP 3-0).