CHAMPIONING CEMA PROTECTION FOR FIRES WARFIGHTERS

Brent Harty

This article is opinion based and assesses existing vulnerabilities in the Fires community, focusing on system protection, PME, and unit training.

CONFRONTING CEMA VULNERABILITIES: FAIL TO PROTECT, FAIL TO FIRE

Cyberattacks and malware targeting critical infrastructure, like our water systems, energy grids, financial institutions, even hospitals, are increasingly common. A quick internet search illustrates the vulnerabilities across civilian and military networks.

While U.S. Fires forces may not face Ukraine's exact challenges, our advanced weaponry and precision ordnance are vulnerable in a Denied, Degraded, and Disrupted Space Operational Environment (D3SOE). Current Fires weapons and C2 systems often lack sufficient hardening against modern CEMA threats, leaving them susceptible to cyber and electromagnetic intrusions.

The question is not if near-peer adversaries will use cyber and electromagnetic offensive capabilities, but when and how severely. Will Fires warfighters be able to mitigate denial and disruption in combat operations absent space-enabled capabilities?

How can leaders prepare their units to fight and win against adversarial CEMA threats?

Realizing the Threat: Cyber, Electromagnetic Attack, and PNT Disruption

One of the most unsettling examples of a capable adversarial cyber threat from a near-peer occurred at the onset of Russia's invasion of Ukraine**.** On 24 February 2022, hackers accessed KA-SAT management servers owned by Viasat, an American communication company, compromising thousands of associated modems. Within hours, this intrusion pushed software updates that deployed the AcidRain hard-drive-wiper malware. A cyberattack of this magnitude against U.S. forces is equally plausible and could potentially cause more destruction than what Ukraine experienced.

Another example of cyber vulnerability comes from outside the battlefield but with direct defense implications. In March 2025, Iran's Bank Sepah—responsible for handling transactions tied to military personnel and defense projects—was compromised in the "Codebreakers" cyberattack. More than twelve terabytes of data, including account credentials and military-related financial records, were exfiltrated from over forty-two million customers. Although not a Fires system, the attack illustrates the broader reality: even organizations tied to national defense can be crippled by determined adversaries. For Fires warfighters, this reinforces the urgency of preparing for cyber and electromagnetic disruptions against their own mission-critical systems.

EW threats across the electromagnetic spectrum (EMS) have also evolved beyond current protections. Jamming—the deliberate use of electromagnetic energy to degrade or neutralize enemy systems—affects radars, navigation, radios, and satellites. Key modernization threats include:

- Digital Radio Frequency Memory (DRFM): Captures and replays RF signals to defeat countermeasures.
- Range Gate Pull-Off (RGPO): Generates false echoes to deceive radar range trackers.
- Velocity Gate Pull-Off (VGPO): Alters radar returns to obscure actual locations.
- Positioning, Navigation, and Timing (PNT) Disruption: Sophisticated spoofing systems increasingly interfere with GPS, degrading aerial and artillery munition guidance.

These evolving threats underscore the need for a Fires force that is not only technologically modern but also intellectually and procedurally prepared to operate in a contested information environment.

Educating the Force: Removing Internal Obstacles

Beyond materiel modernization, Professional Military Education (PME) must match near-peer knowledge on employing nonlethal capabilities. Historically, new doctrine and education lag until more than half the force fields new systems. Consequently, Soldiers, NCOs, and officers often arrive at units underprepared to counter CEMA threats.

Another barrier is the slow revision cycle of the Individual Critical Task List (ICTL). The Critical Task and Site Selection Board convenes only every three years, delaying updates. Fires components conduct their own boards, but gaps persist.

Although the Fires Center of Excellence (FCoE) provides some CEMA instruction, much relies on outside experts rather than organic cadre. This shortfall leaves graduates without adequate awareness or protection skills on arrival to units.

The next step in advancing Fires resiliency lies in institutionalizing CEMA awareness within daily training, doctrine, and leadership—not treating it as a niche or external function.

Innovation in Training: Updating TTPs and TACSOPs

Many units still lack effective, updated TTPs and TACSOPs for CEMA threats. Too often, the default response to cyber or EW attack is to "report to higher" and wait for solutions. This reactive posture is compounded by limited tools for realistic home-station training.

Lessons from Combat Training Centers (CTCs) are also poorly shared. While CALL and the Fires Knowledge Network collect CEMA impacts, dissemination is limited. Units often resort to ad hoc solutions in combat—an unacceptable risk. To prepare formations for LSCO, senior leaders must demand innovation in CEMA protection and ensure that updated TTPs and TACSOPs are fully integrated into unit training.

Senior Leader Impact: Championing CEMA Protection

Senior leaders must require updates to gunnery requirements that incorporate rigorous CEMA protection. These measures should be embedded in train-up and validated during CTC rotations.

Leaders should also leverage PME peer networks to share best practices, ensuring cross-unit exchange of effective TTPs. Additionally, formal mentorship and professional development sessions focused on CEMA will foster innovation and continuous improvement. Only through deliberate leadership can Fires units achieve realistic training in a D3SOE.

Winning in the Future: Emerging CEMA Protection Solutions for Fires

In future conflicts, adversarial CEMA capabilities will only expand in sophistication and scale. Recognizing this, FCoE leaders began working closely with congressional partners and industry innovators to accelerate CEMA modernization within the Fires enterprise. The result was the establishment of the Fires CEMA Protection Team in May 2022, housed in the Fires Innovation Science and Technology Accelerator (FISTA) at Fort Sill. From this location, the team provides accessible, Fires-specific support that bridges institutional gaps between doctrine, education, and materiel development.

The Fires CEMA Protection Team conducts continuous assessments of PME curricula and unit-level training to identify vulnerabilities and recommend mitigation strategies. Since 2023, the team has reviewed more than a dozen unit TTPs and TACSOPs, helping commanders refine their CEMA defensive measures before Combat Training Center rotations. The team also delivers tailored classified threat briefs to officers, warrant officers, and NCOs—ensuring leaders understand both the scale and immediacy of adversarial cyber-electromagnetic threats. This focused instruction directly supports the development of new lesson plans within FA and ADA courses, closing the awareness gap that often exists between the institutional and operational force.

Two emerging materiel solutions exemplify this forward-leaning approach. The Threat Effects Generator (TEG) is a reconfigurable tabletop trainer that replicates real-world electronic warfare attacks in a controlled environment. By visualizing how jamming or spoofing affects their systems, operators learn to identify and respond to electromagnetic attacks using unit-tailored training scenarios before entering combat. The CEMA Resiliency System (CRS) delivers real-time early warning of cyberattacks against Fires systems, enabling operators time to employ mitigating TTPs. Together, these initiatives signal a clear shift from reactive defense to proactive resilience.

While no single program can eliminate CEMA risk, the FCoE's partnership with industry and Congress demonstrates a commitment to equipping Fires warfighters with modern tools and relevant knowledge. By institutionalizing these efforts—through updated PME, realistic training systems, and rapid integration of lessons learned—the Fires community is taking tangible steps toward ensuring dominance in a contested space environment.

Ensuring Fires Dominance

CEMA protection must be a top priority for Fires leaders. Modernized PME, current threat briefs, updated TTPs and TACSOPs, and leader-driven innovation are essential. Emerging tools like TEG and CRS will provide warfighters with tangible training and mitigation capabilities.

While no solution fully eliminates adversarial threats, these initiatives position the Fires enterprise to succeed in future large-scale combat operations against capable near-peer adversaries—ensuring that the U.S. Army's Fires formations remain ready to detect, defend, and deliver in any electromagnetic battlespace.

About the Author

Brent Harty is a member of the Fires CEMA Protection Team at Fort Sill, Oklahoma. A retired Air Defense Artillery Captain, he commanded a Patriot battery and served in multiple battalion and brigade operations roles. Since retirement, he has supported modernization initiatives across the Fires enterprise, including AMD concepts under Army Futures Command.