Fielding c-UAS Effectors at the Speed of Relevance

MDAA Spotlight Series on Iran's Threat and Potential Countermeasures

In our mission to illuminate, elevate, and educate, we are honored to announce a new MDAA series.

The Problem

The current fielding timeline for new counter-Unmanned Aerial Systems (c-UAS) effectors is measured in months to years. In contrast, the threat adapts in days. Attempts to compress the current process have produced limited results because the process itself was designed for a different class of military problem.

The existing acquisition and evaluation model was built to address long-term threats such as tanks, helicopters, aircraft, and artillery systems. Those systems remain relevant for decades, and they evolve slowly enough to justify deliberate requirements generation, extended testing, and comprehensive sustainment planning. This model and process aligned well to threats, and capabilities expected to remain in service over long periods.

UAS present a different operational problem. The threat adapts quickly, proliferates cheaply, and changes often enough that the Department cannot test and evaluate c-UAS systems with an expectation they will remain fixed, decades-long solutions. These realities mean the acquisition and evaluation model's objective has to shift from validating a permanent answer to identifying a safe and useful capability, fielding it quickly, learning from employment, and retesting against the next version of the threat emerging over days.

Every day a capable effector remains in a test queue is a day Soldiers defend with less effective capability than the threat demands. The significance of this shortfall is practical. Delay gives the threat more time to exploit gaps that the force already has the potential means to reduce.

The argument

Reframe the Risk Calculus

The current process treats early fielding as the principal source of risk. That framework reflects an acquisition system designed for enduring platforms, when decisions shape force structure and investment for years. In the c-UAS fight, the relevant risk calculus is different because threat adaptation occurs on operational timelines rather than program timelines.

For a dynamic threat, delay becomes the central operational risk. There are two outcomes of these realities that matter. The force either fields the new effector and learns from operational use, or it delays fielding and accepts continued exposure to the existing threat. If the fielded effector underperforms, the force still gains operational data, identifies limitations, and improves the next iteration. This means that early fielding can preserve defensive capacity while accelerating learning.

Minimum Safety Threshold, Then Field

Once an effector achieves a minimum safety rating, meaning it will not harm the operator and will not create unacceptable collateral risk, it should go to Soldiers. That is the appropriate gateway for a rapidly evolving threat.

The existing acquisition model tests systems with the intent to sustain them for decades. That logic fits long-term platforms. For c-UAS, the requirement is to validate immediate utility against today's threat, and then continue improvement as the threat changes. The implication is that extended operational testing, performance optimization, and iteration become part of the fielding cycle rather than prerequisites that have to be completed beforehand.

The correct sequence is clear. *First*, test for safety and basic utility. *Next*, field the system. *Then*, collect operational data, retest against updated threats, and refine the capability. This means the force could remain aligned to the threat as it evolves rather than waiting for a final answer which will likely be overtaken by events.

The Battlefield is the Test Environment

Real-world operational data provides the most relevant basis for improving capability against a dynamic threat. Controlled testing still has an important role, because it establishes safety, baselines performance, and establishes basic utility. After that threshold is met, operational use provides a faster and more meaningful source of learning.

Soldiers employing the system against live threats will identify failure modes, edge cases, and identify improvement priorities faster than a test protocol built around static assumptions. The implication is battlefield use becomes part of the evaluation process itself. It is no longer served only as the final stage after a lengthy test cycle.

The Department should build a feedback loop accordingly. Field the system after it meets the minimum threshold. Subsequently, collect operational data, retest against the evolving threat, and refine the system for the next iteration. This means the force could sustain relevance against a threat which changes faster than traditional acquisition timelines allow.