

Raven Whispers: The Counter-DRFM Gap

Editor's Note: This article, written by James Spriet, is part of the Raven Whispers series in JED. Many of his Raven Whispers articles are published in the print and digital editions of JED. James also publishes under his Raven Whispers moniker on LinkedIn. This article, ties in with our DRFM cover story, "Creating RF Ghosts – EW Steps Up It's DRFM Game," in the February edition of JED, which you can access with an AOC membership at www.crows.org.

BY JAMES SPRIET

Digital Radio Frequency Memory (DRFM) is the most effective jamming technology ever deployed against modern radar systems. DRFM captures an incoming radar pulse, stores it digitally, manipulates it with precise alterations to range, velocity, or angle, and retransmits it back to the radar as a coherent false return. The radar cannot distinguish the fake from the real because the jamming signal is literally built from the radar's own waveform. It is the electronic warfare equivalent of using someone's own fingerprint to forge their identity.

DRFM-based jammers can generate a range gate pull-off to break missile lock. They can saturate a SAM operator's scope with dozens of false targets. They can defeat wartime reserve modes by digitally generating arbitrary waveforms without ever needing to receive the mode in advance. Every near-peer adversary fields DRFM-equipped platforms. Every modern IADS assumes DRFM capability in the EW threat matrix.

And yet, after analyzing every active Broad Agency Announcement, SBIR topic, and special notice related to Electronic Warfare across DARPA, AFRL, ONR, and the Naval Warfare Centers, I found no dedicated program specifically targeting counter-DRFM technology.

Zero.

The Gap

The absence is conspicuous. Programs exist for cognitive EW, adaptive waveforms, distributed sensing, AI-enabled threat classification, and spectrum situational awareness. AFRL's Kaiju program dedicates \$150 million to machine learning for electronic warfare. DARPA's I20 office funds transformative AI for the information domain. The Navy funds dynamic scheduling for software-defined radios. Counter-UAS EW receives attention from every service.

But counter-DRFM? The phrase appears nowhere in current unclassified solicitations. The closest language is buried in generic "advanced threat defeat" technical areas that could mean anything from noise jamming to directed energy.

This creates three possibilities, none of them comforting.

Possibility one: Counter-DRFM is handled entirely in classified programs. This is plausible. The techniques required to defeat DRFM reveal what radar waveforms and processing methods we consider vulnerable. Discussing counter-DRFM in the open tells adversaries which deception techniques we prioritize defeating, thereby revealing which techniques are working. Classification makes sense from an OPSEC perspective. However, it is crucial to balance the need for operational security with the advantages of industry engagement. While certain specifics must remain classified to maintain strategic advantage, fostering a collaboration with industry can drive innovation and preparedness. Yet, the current classification means the broader industrial base has no visibility into requirements, no opportunity to propose solutions, and no market signals to invest in IR&D for counter-DRFM research.

Possibility two: DoD has accepted DRFM as an unsolvable problem. This is darker but not unreasonable. The fundamental

challenge with DRFM is that coherent jamming exploits the physics of radar itself. The deceptive signal matches the radar's waveform because it is the radar's waveform, captured and replayed with modifications. Defeating this requires the radar to authenticate its own returns, which demands either secret waveform features the jammer cannot replicate or processing techniques that detect subtle inconsistencies. Both approaches have limits. A sufficiently advanced DRFM with low latency and high fidelity can track most agility techniques. If the classified assessment is that counter-DRFM is a losing game, then not funding it publicly is a rational allocation of resources.

Possibility three: Counter-DRFM is embedded in vague solicitation language without explicit mention. This is likely but problematic. Terms like "advanced electronic protection," "adaptive radar processing," and "cognitive ECCM" could encompass counter-DRFM work. But vague language produces vague proposals. Without specific technical requirements, proposers guess at what the government actually wants. Some guess right. Most guess wrong. The result is wasted effort on both sides and slower progress toward fielded capability.

What Counter-DRFM Actually Requires

The technical community knows what counter-DRFM looks like. The AOC offers courses on it. Academic papers describe the techniques. The methods fall into several categories.

Waveform agility: Radars that rapidly change pulse parameters, frequency, or coding make it harder for DRFM to maintain coherence. If the jammer doesn't know what the next pulse looks like, it cannot generate a convincing fake.

Pulse diversity techniques: Using different pulse shapes, block coding, or orthogonal waveforms across a coherent processing interval creates signatures that DRFM cannot easily replicate without introducing detectable artifacts.

Statistical discrimination: DRFM returns have subtle differences from real returns. Phase noise characteristics, timing jitter, and amplitude variations can betray the jammer if the radar's processing is sophisticated enough to detect them. However, the technique is not without its drawbacks. The increased sensitivity required for effective discrimination can lead to higher false-alarm rates, which may result in unnecessary defensive actions and resource allocation, impacting overall system efficiency. This trade-off is a critical factor in the practical application of statistical discrimination methods.

AI and machine learning: Neural networks can learn to recognize DRFM-induced anomalies that rule-based processing misses. This is where cognitive radar meets cognitive jamming in a machine-speed adaptation battle.

Polarization discrimination: DRFM systems typically replay signals with the same polarization as the signals they received. Radars that transmit one polarization and analyze returns across multiple polarizations can detect the absence of expected scattering diversity.

None of these techniques are classified. All of them could be developed, tested, and refined under unclassified BAAs. The fact that no such BAA exists suggests either deliberate omission or institutional blind spot.

The Opportunity

For the industry, the counter-DRFM gap represents both risk and opportunity.

The risk is obvious. Investing in IR&D to counter DRFM without a clear procurement pathway is a gamble. If the work is happening in classified channels, your unclassified proposal may be redundant or may reveal that you don't have access to the real requirements. If DoD has written off counter-DRFM, your proposal addresses a problem nobody wants to solve.

But the opportunity is equally real. A proposal that explicitly addresses counter-DRFM detection and mitigation will stand out precisely because no one else is directly tackling it in unclassified space. Program managers frustrated by the absence of tailored solutions may welcome a proposer who names the problem directly. The Kaiju program's technical areas include "advanced threat defeat," language broad enough to encompass counter-DRFM work if the proposer frames it correctly. ONR's electronic protection research could accommodate counter-DRFM under existing authority.

The key is framing. Don't propose counter-DRFM as a standalone problem. Propose it as an instantiation of cognitive ECCM, adaptive radar processing, or AI-enabled electronic protection. Use the terminology the solicitations use while solving the problem they don't name.

The Bigger Picture

The absence of dedicated counter-DRFM funding reflects a broader pattern in DoD EW investment. Programs focus on offensive capability, spectrum awareness, and distributed effects. Defensive electronic protection receives less attention, less funding, and less specificity. This makes sense if you assume air superiority and spectrum dominance. It makes less sense if you assume contested airspace against adversaries with mature DRFM capability.

Adversary platforms are fielding increasingly sophisticated coherent jammers. AI-enabled DRFM that adapts in real time to radar countermeasures is not theoretical. It is in development now.

The question is whether counter-DRFM is a problem DoD is solving quietly, a problem DoD has accepted, or a problem DoD hasn't fully recognized. The funding record suggests the answer, but the funding record may not tell the whole story.

For now, the gap remains. And gaps create opportunity for

those willing to fill them.

Follow "Raven Whispers" on LinkedIn for more EW/ISR insights and articles. Email jamesspriet@ravenwhispers.com for topic suggestions, inquiries, collaboration, analysis requests, or feedback.