FTCN Replay: How AI is Rewriting the Rules of EW

Artificial intelligence is reshaping how militaries compete for control of the electromagnetic spectrum – and the US may not be moving fast enough to keep pace.

On the most recent episode of [From the Crows’ Nest](), host Ken Miller was joined by Dr. Karen Zita Haigh, a leading expert in cognitive electronic warfare and embedded AI, who warned that institutional barriers are slowing adoption of technologies that could prove decisive in future conflicts. The episode took place against a backdrop of ongoing operations against Iran and emerging lessons from the Russia-Ukraine war, including reports of Ukrainian forces hijacking Russian jamming signals to target command centers.

What Cognitive EW Actually Means

Haigh began by drawing a clear line between artificial intelligence as a broad field and the specific tools most people associate with it.

“The media would like you to believe that machine learning equals AI,” she said. “In fact, there are lots of people who use the term AI and ChatGPT synonymously. To me, ChatGPT is a tool, but it’s not AI. AI is a field of study and machine learning is an area within that.”

A cognitive EW system, she explained, goes several steps beyond a standard AI-enabled system. Rather than applying a static model – like the kind used to scan luggage at an airport – a cognitive system continuously learns from its own actions in real time.

“A cognitive EW system understands and predicts the electromagnetic spectrum,” Haigh said. “It makes goal-directed decisions to improve the performance of that EW system, and it learns from its own actions. And all of that has to happen at mission-relevant time scales with minimal human supervision."

No Plan Survives Contact, But AI Can Adapt

One of the episode's central themes was the gap between pre-mission planning and battlefield reality. Haigh described how cognitive systems can close that gap by continuously replanning as conditions change.

She used a drone swarm as an example: a commander may know going in that 10% of platforms will be lost, but not which ones. The system must be capable of redistributing tasks on the fly among surviving assets.

"The definition of idiocy is to do the same thing over and over again and expect a different answer," she said. "I don't want my EW system to be an idiot. I want it to say, that didn't work – do something else next time."

Beyond expected losses, Haigh said systems also need to handle complete surprises – moments that require scrapping the current plan and rebuilding from the current position. Continuous monitoring of whether intended effects are actually occurring is equally critical, she noted, and an area where military operations have historically lagged.

Protecting Algorithms From Manipulation

The conversation also explored vulnerabilities in AI models themselves, specifically, whether adversaries could manipulate the data or algorithms underpinning military decision-making.

Haigh acknowledged no system is foolproof in an adversarial environment, but pointed to data diversity as the most effective mitigation. She referenced a well-known 2017 study in which researchers fooled a stop-sign recognition model simply by placing sticky notes on the signs – a failure she attributed to a narrow training dataset.

She also raised a less commonly discussed protection method: homomorphic encryption, which keeps input data and all intermediate calculations encrypted throughout processing.

“Unless you can break my encryption key, it means nothing to you,” she said.

The Bigger Barrier: Bureaucracy, Not Technology

When asked what challenges keep her up at night, Haigh was direct: the hardest problems are not technical.

Acquisition processes, contracting timelines, and institutional siloes between military branches are slowing progress more than any gap in the underlying science, she said. The US has largely failed to adopt NATO’s CESMO standard for real-time spectrum observation sharing across coalition forces – and many American practitioners aren’t even aware it exists.

“The permissions to share are more difficult than the technology to share,” she said.

She also challenged the widespread assumption that AI systems require high-powered GPU hardware to operate effectively.

“You can right-size that AI model for the device you have,” she said, noting that even large language models are increasingly being adapted for small microcontrollers.

Haigh closed on a note of cautious optimism, pointing to the rapid innovation spurred by the Ukraine conflict as a model, while expressing hope the US doesn’t need a similar shock to accelerate its own modernization.