DOD Must Prioritize EP to Achieve EMS Superiority

During the AOC 2021 Virtual EMS Summit in April, Mr. David Tremper, SES, EW Director, OUSD(A&S)/A/P&WPM, spoke to the Electromagnetic Warfare (EW) challenges currently facing the DOD at the force level. Tremper particularly noted the insufficient focus on Electromagnetic Protection (EP) within DOD EW, which contributes to and intensifies today's major Electromagnetic Spectrum Operations (EMSO) challenges.

Tremper said, "[EP] happens outside the purview of the DOD EW community, and very often the way we learn about EP features is when they fail operationally and they show up back in our office [in need of a solution]."

"Passive sensing and netted passive sensing is becoming more and more important every day because the more we emit, the more we become targets," Tremper said. "So we have this conundrum that we can either emit high-power signals to get exquisite battlespace awareness, or we can turn off those emissions and protect ourselves from passive targeting."

"There has been a recognition, as we have talked about connective tissue across spectrum systems, spectrum programs and the acquisition of spectrum capabilities, that EP has been falling through the cracks," he said. "The textbook defines EW as including EP, but the way that we [at DOD] manage EW, EP is not a part of EW. It's in the other spectrum-using systems."

The challenge is not, however, confined to acknowledging the importance of EP within the DOD, according to Tremper. It lies also in creating a firm understand throughout the department of what EP means.

Tremper said, "In the Department, I took for granted that people understood what the term 'electronic protection' meant,

and what I have discovered is that … the perception is that electronic perception means platform protection. Platform protection is actually what we would call defensive electronic attack."

Electronic Attack (EA) and Electronic Support (ES) are currently the focus of DOD EW capability and systems development, according to Tremper. The onus of EP management, however, has been placed on non-EW RF system developers.

The DOD must, Tremper said, begin prioritizing and taking ownership of EP in order to ensure spectrum using systems (radar, communications, GPS, IFF, etc.) can function properly in a congested and contested EMS before they are fielded. Indeed, the entire concept of EMS superiority is dependent upon effective EP, according to Tremper.

"When we talk about EM Dominance and we talk about EM Superiority, Electronic Protection is critical. It's critical that all of our spectrum-using systems are capable and superior and can maintain resilience within a complex EMS environment."

Tremper noted that there are five "levels" to ensuring EMS system survivability. The first, awareness, was satisfied in 2018, according to Tremper, with the 2018 JCIDS Manual of Operations, which outlines the importance of EMS survivability. The second level, advocacy, was achieved through the publication of the latest EMS Superiority Strategy (EMSSS), which maintains a focus on EMS survivability.

The next three levels include verifying EMS systems are survivable via thorough, representative testing; enforcing survivability requirements via authority streamlined processes, actionable assessments and punishable non-action; and achieving survivability in systems and operations. Each of these remaining three levels cannot be achieved without DOD involvement in and understanding of EP, he said.

Artificial Intelligence (AI) and Machine Learning (ML) technology can assist in bolstering EP, according to Tremper, but that contention comes with its own set of complications. While AI and ML technology may allow for more effective EP capabilities in fielded platforms and systems, that technology depends heavily on acquiring real or realistic data from specific EM operating environments that is needed to train the AI-based systems. That EMS data is a commodity that's difficult to acquire in theater and slow to synthesize in training settings.

These data acquisition issues, however, are actively being addressed by industry through a variety of methods. One of the more promising techniques, according to Tremper, is the use of "operationally deployed digital twins as training environments for algorithms."

These digital, or "virtual," twins are AI-based systems deployed parallel to (and often physically collocated with) an operational radar or communications system, for example. The digital twin performs the same functions as the actual system, but in a virtual mode – without effecting any changes to their environment or connecting with other systems in on the weapons platform. A virtual twin acts, Tremper said, as a "petri dish for new technology," by creating an environment where a learning algorithm can be "parked" to have access to all sensor data and operators' interactions with that data. This allows the virtual twin to learn while it's actively deployed rather than in a test or training setting.

The usefulness and viability of the virtual twin concept is that the "twin" system does not, at any time, have direct access to the weapons system. "It can build a firewall away from the combat system that allows it to avoid … the information assurance requirements that would be levied on it if it showed up in the combat system," Tremper said.

The process for getting approval to alter or add to a weapons

system is lengthy and onerous, which makes virtual twins ideal, according to Tremper. A virtual twin is incapable of controlling a weapons system but can still see the information available to that system, effectively "firewalled" from combat capabilities. This allows an algorithm to be used and altered in the field as needed, rather than going through an approval process for each algorithmic change.

"When you think about that in terms of acquisition, it flips our acquisition process on its head," Tremper explained. "There's a possibility that the way we acquire AI and ML is not that we train it in a lab … with a bunch of computers, but that we deploy it – that we deploy untrained algorithms right at the beginning, and they learn 24/7, in the field, using real data, real operations, as a mechanism to achieve operator-level proficiency and beyond." – *H. Swedeen*