A force in flux: Military adjusts to emergent domains of warfare

Posted on May 2, 2017 by Mark Pomerleau with 1 Comment



The Army — and the military writ large — is undergoing the initial stages of a fundamental change in thinking, organizing and, ultimately, fighting.

Fifteen years of continuous war against technologically inferior enemies that has provided a window for adversaries to observe U.S. tactics, and the advent of new and cheap technologies to achieve great effects are factors that have forced the military to realign under what it generally calls multi-domain battle.

Multi-domain battle seeks to integrate operations and coordinate seamlessly across the five domains of war — air, land, sea, space and cyber — as opposed to the antiquated domain-specific approach to solving problems.

Emergent domains, such as cyber and space, and adversarial use of such battlefields, has the force rethinking how it will organize conventional units and at what level to incorporate skill sets within these war-fighting environments.

"This is probably the thing we are focusing on the most right now and gives us the largest challenge," Gen. David Perkins, commander of the Army's Training and Doctrine Command, said in March at the Association of the U.S. Army's Global Force Symposium.

Highlighting cyber as one example challenging the current force structure organization, Perkins noted how today a force thousands of miles away in cyber can be committed to the close fight, raising questions such as who would "own" that fight in the traditional sense.

Another challenge that will arise as the military looks at the battlefield framework of multi-domain battle, Perkins explained, is that the force as a whole tends to be geographically separated. Effects might occur at the location, but at different times, he added.

Perkins wondered how this can be synchronized when it's all occurring at the squadron level.

"There could be cyber activity going on at the squad, and what are the authorities? The question really is: What is the battlefield framework and what are the authorities? We don't have all the answers yet," he said.

Reorganizing military units

"We need to reevaluate how [the U.S. armed forces] fight," David Johnson, senior fellow at the Center for Strategic and Budgetary Assessments, said at the AUSA conference. He asked what key capabilities are needed to keep above the brigade and offered that things like electronic warfare can't be fielded at the brigade level.

The commanding general of the Army's Maneuver Center of Excellence told C4ISRNET that his organization must collaborate with the Cyber Center of Excellence to organize maneuver elements and echelons to incorporate soldiers with cyber and EW skill sets.

"What we said in the concept is brigades are going to have to be semi-independent; and if they are independent and cannot communicate, what tools does a brigade need to self-sustain and secure itself?" Maj. Gen. Eric Wesley said. He added that the service is still working through the authorities, policy changes and structure.

Given that all domains will be contested in the future, "I have to have a component from cyber within the brigade combat team so they can fight and win," he said.

Wesley said the thinking is that cyberspace — and maybe EW to a degree — has to be managed, for the most part, at the echelons above brigade level because a brigade commander doesn't have the bandwidth to do all that activity.

"All we're saying is they have to be able to be cognizant of how to maneuver through those domains to be effective."

To that end, the Maneuver Force Modernization Strategy, which will be finalized in the summer, will say that cyber needs to be incorporated into the formation, and the force will have to figure out how to do this, Wesley said.

"I think reconnaissance is probably the most you'll see at the brigade level — cyber reconnaissance," he said.

The Army's cyber components currently are running experiments at the National Training Center aimed at getting this right. The Cyber and Electromagnetic Activity Support to Corps and Below pilot is gaming how and at what levels to integrate cyber and EW soldiers into maneuver forces.

This isn't just an Army problem. Brig. Gen. Julian Alford, commanding general of the Marine Corps Warfighting Laboratory, said at the AUSA symposium that Marines also are very focused on this problem. What is the unit of measure? Is it a company? Can the Marines fight more distributed? Can units perform and exact effects from different parts of the world? Alford said these are the types of questions they're examining.

A major discussion point under the guise of multi-domain battle is the need for cross-domain fires — the ability of effects to be initiated in one domain and reverberate in others.

"There's a huge opportunity for effects being generated or felt even at the tactical edge of the battlefield, but maybe not necessarily generated at the tactical edge but definitely felt at the tactical

edge," Maj. Gen. Brian McKiernan, commanding general of the Army Fires Center of Excellence and Fort Sill in Oklahoma, told C4ISRNET.

McKiernan asserted that the Cyber Center of Excellence is the chief integrator of cyber capabilities from a tactical, forward-deployed and more strategic remote location standpoint.

Why the shift?

While the nature of war remains the same, the character of war is experiencing change, with catalysts such as social media, cyber and information operations, and small, commercially available UAVs, all of which lead to an increasingly lethal battlefield where all domains will be contested and congested.

There is also the common talking point that the U.S. is increasingly outmanned, outgunned and outranged — both in capability and capacity in a lot of ways.

While the U.S. possesses much greater capabilities and doctrine when taken by themselves, the issue is that they have been developed and integrated in a siloed fashion.

"So we did this Russian new-generation warfare study — that's what essentially spotlighted for us that there were old technologies being used in new ways and new technologies being used in new ways, and the combination of those are creating gaps that we do not have solutions for," Maj. Gen. Bo Dyess, acting director of the Army Capabilities Integration Center at TRADOC, told reporters during the AUSA symposium.

The study was commissioned in February 2016, and the author traveled to Ukraine to observe Russian activities there.

"Even a most casual look into what Russia is doing in eastern Ukraine today tells us insights into what a multi-domain battle environment will look like," according to Maj. Gen. Duane Gamble, the commanding general of 21st Theater Sustainment Command. "It will require us to operate and sustain operations in an unforgiving lethal environment, one in which our Army [has] not operated in since World War II or some of the battles in Korea."

Dyess also noted that the Army is learning from the Russian new-generation warfare study.

"This forms the base of our thinking about the multi-domain battlefield of the future," he said.

The pacing threats of near-peer adversaries are also driving the Army to reinvigorate some capabilities it divested in the past decade or so.

"We don't want to be surprised on a future battlefield ... in order to not be surprised on a future battlefield we have to question the assumptions that we have, like air supremacy or air superiority," Dyess told reporters. "We assume that we had that and therefore we took actions inside the Army to cut our field artillery, to do away with EW inside the Army as a capability, and now we're finding that those capabilities did not go away on our threat — enemy, adversaries — at the near-peer level. We've just been focusing on a different thing the last 15 years, and appropriately so."