Joint All-Domain Operations

LT GEN JAMES B. HECKER, USAF

In the struggle for survival, the fittest win out at the expense of their rivals because they succeed in adapting themselves best to their environment.

—Discussion of Charles Darwin’s views

Ritchie R. Ward, The Living Clock, 1951

The Department of Defense’s transition to Joint All-Domain Operations (JADO) as the doctrinal framework for future strategic competition captures and codifies truths about war fighting that may be obvious in the comfort of 20/20 hindsight. The idea that the application of force in one domain may affect outcomes and capabilities in another has been an element of American military thought for more than 240 years, for example the Battle of Yorktown, 1781. B-17s conducting antisubmarine patrols during the Battle of the Atlantic to protect Allied shipping in World War II engaged in multidomain operations: in this case, air assets were used to detect and prosecute German U-boats that harassed merchant convoys delivering supplies and troops to the European theater of operations. Likewise, carrier-based aviation naval and ground-based fighters performing close air support for soldiers and Marines on the ground in Korea and Vietnam delivered firepower in support of land objectives.

In contrast, however, JADO marks a dynamic transition in the conceptualization of maneuver warfare characterized by complexity, speed, and precision. Success in JADO will require sophisticated combinations of synchronized domains far beyond what has been historically demonstrated. Additionally, the rapid technological changes we have recently experienced and the ever-growing dependence on the electromagnetic spectrum will have an unforeseen impact on the effectiveness of military operations in all five recognized domains—air, land, sea, cyber, and space.

Assumptions and practices that guided American military thought from Desert Storm to the wars in Afghanistan, Iraq, and Syria may not be valid in future strategic competition against adversaries using advanced technologies. The notion
that future conflict will resemble Operation Desert Storm, with its months of buildup in regional sanctuaries unchallenged by an isolated regional adversary, has been invalidated by Russia’s gray-zone operations in Syria and Ukraine, and in perpetual challenges in the cyber and space domains. Regional access to secure operating locations is no longer a given.

Threats to access in the electromagnetic spectrum, as well as the integrity of data down to the individual bit level, challenge our ability to communicate with and command and control our forces. Ransomware attacks against American commercial and civil targets offer hints about the potential impact of dedicated adversary actions against infrastructure and communications. As we continue to rely on access to information across the space and cyber domains, potential vulnerabilities multiply by the thousands. The decisive actions in future wars may be completed within the first 30 seconds of conflict; the outcome on the battlefield may not manifest until weeks or months later.

The release of Air Force Doctrine Publication 1 earlier this year recognizes the challenges present in contemporary strategic competition in its reframing of how Air Force personnel must consider airpower. The key tenet of Air Force doctrine, dating back to its roots in the Army Air Force, is that airpower’s true potential is realized in command relationships of centralized control and decentralized execution. The changing threat environment and the realization the Air Force needs to change to stay relevant, means that we now “execute mission command through centralized command, distributed control, and decentralized execution.” The addition of both mission command and distributed control are integral to the service’s continued relevance in the Joint all-domain battlespace.

Success in the Joint all-domain environment at the tactical, operational, and strategic levels cannot be guaranteed by massive system investments and recapitalization efforts. Nor is it enough to accept as an article of faith that artificial intelligence will save the day in future conflict. Unmanned aerial vehicle swarms may one day be able to demonstrate new and novel capabilities, but turning these ideas into capabilities that demonstrate value in today and tomorrow’s fight is imperative. It is neither easy nor quick to do so. We deliver air and cyberspace capabilities every day for the nation while also learning how to do so in more effective ways. As an organization, the Air Force is unable to take a sabbatical for a decade to figure out the future. This means that research, modernization, and current operations compete for attention, manpower, and money and the emphasis on flexibility and rapidity is precedent in today’s era of competitiveness.

The articles in this volume do not solve JADO for the Department of the Air Force. Rather, they capture contemporary thoughts and insights about different aspects of operating and fighting in Joint, multidomain environments. These
practitioners begin to address the deep work required to advance JADO from a conceptual framework to true mission capability for Air Force personnel, Guardians, our Joint partners, and our Allies and partners around the globe. Mission command and distributed control will be inherent components in future military action. Both the Air Force and the Space Force need to define how we will embed these elements into our institutions, structures, and processes. While new hardware and software are essential elements of future operational realities, the thoughts and ideas that accompany them will be just as important in creating relevant and decisive capabilities for the nation.

Lt Gen James B. Hecker, USAF

Commander, President, Air University