

The All-Domain Protection Story

By Mr. Damon M. Yourchisin

Previous studies exposed protection from threats that create standoff in all domains as a critical Army challenge and, therefore, identified a requirement that was coined “all-domain protection” by the protection community. This drove the creation of U.S. Army Futures Command (AFC) Pamphlet (Pam) 71-20-7, *Army Futures Command Concept for Protection*,¹ signed by Lieutenant General Scott D. McKean, Director, U.S. Army Futures and Concept Center, Fort Eustis, Virginia, in April 2021. The concept focuses on the integration and synchronization of protection activities required to enable, penetrate, disintegrate, and exploit activities as the protection warfighting function (WFF) contribution to the Army Operating Concept of multi-domain operations (MDO). The three “big ideas” enabling all-domain protection are—

- Deny enemy freedom of action through protective counteractions.
- Enable access in depth.
- Preserve essential capabilities, assets, and activities.

The Maneuver Support–Capabilities Development and Integration Directorate (MS-CDID) and the Maneuver Support Center of Excellence (MSCoE), Fort Leonard Wood, Missouri, are responsible for protection WFF synchronization.

The Problem

Protection as a WFF is currently a blind spot for the Army—specifically, for commanders at every echelon. There is no common understanding of what all-domain protection entails—or even what it means. If MDO calls for the ability to enable, penetrate, disintegrate, exploit, and compete in all domains, then all-domain protection can be expected to be an extensive and intricate component of MDO. This does not describe our grandfather’s protection; protection in MDO is very different than it has been for more than 20 years.

If the output of air-land battle is the coordination and synchronization of air defense into protection planning, then the MDO output would be the coordination and synchronization of all-domain protection and defense. In MDO, protected maneuver and fires generate combat power.

The Solution

To describe the Army protection concept, MS-CDID took an inverse approach to convergence. The approach centered around enabling MDO formations in competition and conflict by denying enemy freedom of action through the following protective counteractions in all domains:

- Enabling access in depth.
- Establishing and retaining dispersed support areas.

- Shaping movement corridors.
- Preserving essential capabilities (formations, assets, and activities).

Ultimately, the Army must set security conditions in support areas at echelon to enable maneuver and fires to close with and destroy the enemy.

Protection in MDO

The MS-CDID approach is broad; however, when fully integrated and synchronized with other future contributors to the function, this approach will reduce the cumulative effects of adversary standoff on our formations, improve our tempo, and ultimately enable credible responsiveness across strategic and operational distances to deter, deny, or quickly reverse the adversary’s *fait accompli* objectives.

Operational Environment Threats

Predicted means and methods of future threats on the expanded battlefield have forced the Army to examine its blind spots and understand how threat standoff degrades its operational responsiveness through effects in all domains. The connective tissue that has been lost with maneuver and the other WFFs over the past 20 years or more must be regained to facilitate the complete modularization of enabler force structure in order to accomplish MDO. The expanded battlefield framework, the tempo, increased distances, and maneuver in all domains provide the context.

Challenges

Today, the homeland strategic support area is contested, even during competition. Movement from fort to port does not take place in a permissive environment and is no longer a foregone conclusion. As operational and tactical support areas expand, area, route, and movement corridor security are required at much greater distances and speeds against a much more lethal threat.

Results of experimentation focused on 2040 also predict that the battlefield of the future will be transparent to both blue and red forces. This poses unique protection challenges for forces; if forces can be detected or seen, then they can be hit by enemy fire.

In the hyperactive space of the close area, situational understanding of commanders at every echelon will be critical in ensuring that proactive, risk-based decisions are made before entering the hazard area. In deep maneuver and fires areas, the ability to deny the enemy freedom of action on our terms across all domains becomes critical.

Senior Army leaders understand the criticality of addressing protection challenges as part of the essential elements of

combat power. The key to building combat power is through protected maneuver and fires. Integration and unity of effort across all protection-related activities render the whole greater than the sum of the parts. Over the next several years, Army experimentation will be focused on addressing learning demands to fully achieve all-domain protection.

Experimentation Planning

Experimentation follows the general path of presenting concepts/required capabilities at the—

- Annual virtual MS-CDID Protection Science and Technology Forum (to focus efforts on protection needs).
- Maneuver Support, Sustainment, and Protection Integration Experiment (MSSPIX) (to identify specific capabilities that meet Army requirements and assess them through a Soldier touch point).
- Project Convergence/Joint Warfighter Assessment (to demonstrate how these capabilities function as a system and in operational context).

This process leads to the production of requirements documents for the appropriate capabilities to meet Army protection needs for 2035 and beyond. All-domain protection is critical to the ability of the MDO force to deny enemy actions; enable access for friendly operations; and protect critical capabilities, assets, and activities.

Key Insights

For the Army to understand its protection requirements as part of the joint force, it must consider protection as a cultural part of its everyday existence. It must develop standards and provide training for conducting assessments for all protection tasks. With a robust, multidomain capability set that includes camouflage, concealment, and decoys, the Army can make significant improvements in protecting the force during all phases of the competition continuum; and through deception, the Army can make significant improvements in protecting the force and enabling facilities (including supply/command and control nodes). Additionally, after several analysis sessions and senior-leader engagements, the following insights have become apparent and can serve as the basis for further gap analysis discussions:

- Without a joint protection concept to define it, the meaning of operational dispersion is unclear.
- The atmospheric littoral space represents a protection challenge for everyone who is not inside an air defense artillery bubble.
- It is time to update the Army Universal Task List.

Operationalizing protection and fully realizing the AFC Concept for Protection 2028² require that MSCoE assess the current state of protection across the WFF, develop new protection solutions, and educate the force. This work involves lead personnel from AFC and the U.S. Army Training and Doctrine Command as well as from across multiple proponents outside of MSCoE. Many aspects of current and ongoing doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) domain efforts operationalize the key protection concept

themes of deny, enable, and preserve; some such aspects include—

- **Protection assessment.** Protection assessments must span echelons ranging from the Soldier to the Army service component command, compare aspects of protection against MDO expectations, and encompass each of the DOTMLPF-P domains. The All-Domain Protection Capabilities-Based Assessment, a priority effort led by MS-CDID, will continue through Fiscal Year 2023. The U.S. Army Combined Arms Center, the *Army Lessons Learned Annual Plan*,³ and the virtual Army Lessons Learned Forum facilitate engagement and integration of protection learning demands into relevant exercises. Internal experimentation, such as that conducted in the Maneuver Support Battle Laboratory corps protection cell tabletop exercise and at MSSPIX, combined with external experimentation such as that conducted at the Joint Warfighting Assessment 2022, continue to allow for the exploration and assessment of new, advanced protection concepts, technologies, and units. After action reviews on real-world events significantly contribute to protection assessments. Learning events such as these provide input for the development of DOTMLPF-P solutions and help educate the force.
- **Protection development.** Field staffing of the initial draft revision of Army Doctrine Publication (ADP) 3-37, *Protection*,⁴ began in August 2022, and publication of the revised version is scheduled for summer 2023. Practitioners can expect the revised version to help improve integration with the operations process, expand descriptions of tools and estimates for proactive protection planning and execution, and describe additional enabling activities. Organizationally, protection cells in echelons above brigade headquarters are seeking a massive expansion to meet the planning needs for all-domain protection in depth. MSCoE and the U.S. Army Cyber Center of Excellence, Fort Meade, Maryland; the U.S. Army Fires Center of Excellence, Fort Sill, Oklahoma; the Army Protection Program; and others are bringing exciting new protection capabilities and capacities online. Future developments in other DOTMLPF-P domains include the development of a protection additional skill identifier and the creation of various protection job aids.
- **Protection education.** The capstone of operationalizing protection is protection education. Equipped with information from the multicomponent Protection Integrator Course and a critical task selection board, pilots of the Protection Integrator Course continue to lead to a full Army Training Requirements and Resources System listing; beginning in Fiscal Year 2025, the successful completion of a 2-week course will result in additional skill identifier for attendees. The Protection Integrator Course targets protection cell leaders in echelons above brigade headquarters, as well as their supporting elements and staff, to apply protection in depth in all domains. The U.S. Army Combined Arms Center, Fort Leavenworth, Kansas, and MSCoE are teaming up to explore the possible development of an Intermediate-Level Education protection elective at the U.S. Army

(Continued on page 6)

challenged by cyber defense measures, signature management, and information security—three areas that required significant integration in the protection working group.

The exercises provided an opportunity for the force to observe how the protection warfighting function has changed over time, from a specific emphasis on force protection to an expanded emphasis that includes operational security and counterintelligence in the irregular-warfare environment. Inherent to irregular warfare is the application of effects that disrupt, degrade, illuminate, and facilitate human networks and infrastructure to meet a desired end state. The role of the protection cell in these effects is twofold. First, intended results of these effects on the target will potentially affect the surrounding friendly network and infrastructure. For example, effects that inhibit the capabilities of the target could also equally affect friendly capabilities, in addition to illuminating the ODA itself. If a special operations unit of action is operating in a denied area, how can it ensure space and distance so that the origin and intent of the ODA is not discovered? The second role of the protection cell in the application of effects is in providing input on the protection capabilities of the target and exploiting its vulnerabilities.

In irregular warfare, tactical special forces units of action operate mostly within a small footprint, with multiple partner units dispersed across several geographical areas. The dispersion alone contributes to effective force protection, but integrating counterintelligence can assist in protection efforts. Counterintelligence activities can establish a formal liaison with host nation intelligence, law enforcement, and security forces to assist with operations while also creating access, space, and distance for the special operations forces units of action in the area.²

Ultimately, protection in irregular warfare is similar to protection in conventional warfare in that it is the process of identifying and assessing threats to determine risks and develop mitigation actions. However, units of action operating in irregular warfare start their operations in what are already high-risk, denied areas. Neither traditional forces nor traditional protection measures can be applied in this environment. Rather, protection in irregular warfare requires creative and layered solutions that align with the supported operation. Exposing protection mitigations potentially exposes the force being protected, which can ultimately escalate an entire theater from competition to crisis or from crisis to conflict.



Endnotes:

¹Army Doctrine Publication (ADP) 3-05, *Army Special Operations*, 26 August 2019.

²Ibid.

Captain Gasvoda is the plans and operations officer for the Military Police Security Force Assistance Team, Office of Special Warfare, 1st Special Forces Command. She holds a bachelor's degree in biology from the University of Colorado, Colorado Springs, and is currently pursuing a master's degree in criminal justice-forensic science from Saint Leo University, Florida.

(“The All-Domain Protection Story,” continued from page 4)

Command and General Staff College, Fort Leavenworth, and the creation of a commander's guide to protection. Protection Net, located on milSuite at <<https://www.milsuite.mil/community/spaces/apf/protectionnet>>, is the collaborative work forum for the protection community. Finally, MSCoE is engaging the broad protection community through quarterly protection WFF operational planning teams and semiannual protection warfighter forums for echelons above brigade protection cells and the operating force.

• **Protection materiel.** In driving forward to ensuring an MDO-capable force in 2030 and designing the force of 2040, there are three big MS-CDID/MSCoE ideas that could have an immediate effect:

- Automation in breaching and chemical, biological, radiological, and nuclear hazard assessment needs to be fast-tracked.
- Artificial intelligence support tools for synchronizing protection at echelons must be pursued.
- The critical space where protection and deception intersect in offsetting vulnerabilities must be initially understood and exploited through next-generation obscuration.

Conclusion

All operationalization efforts are focused on aligning outputs to support the Futures and Concept Center/Combined Arms Center integrated priority list, which ensures that all modernization stakeholders work on the Army's big problems (specifically, in the area of future protection functional concepts/regimental modernization strategies) and link them to the Total Army Analysis/Strategic Portfolio Analysis review/program objective memorandum processes in order to execute in terms of personnel, funding, and timing. This approach will support delivering the Army of 2030 and designing the Army of 2040 and beyond.

In order to provide unity of effort at echelon and to conduct all-domain protection with the organizations and capabilities needed to preserve our critical capabilities, assets, and activities (including control of our division and corps rear and support areas), MSCoE ultimately serves as the proponent for the protection WFF.



Endnotes:

¹AFC Pam 71-20-7, *Army Futures Command Concept for Protection*, 7 April 2021.

²Ibid.

³Executive Order 193-22, *Army Lessons Learned Annual Plan—Fiscal Year 2023*, Headquarters, Department of the Army, 28 July 2022.

⁴ADP 3-37, *Protection*, 31 July 2019.

Mr. Yourchisin is the deputy director for MS-CDID, Futures and Concepts Center, AFC, Fort Leonard Wood. He holds a bachelor's degree in biology from Gannon University, Erie, Pennsylvania, and master's degrees in environmental science and engineering from Baylor University, Waco, Texas, and environmental management from Webster University.

Protection