

The Protection Warfighting Function in Irregular Warfare

By Captain Emily A. Gasvoda

1st Special Forces Command (Airborne), Fort Bragg, North Carolina, is the world's premier irregular warfare force. 1st Special Forces Command units of action operate across geographically dispersed locations in hostile, denied, or politically and/or diplomatically sensitive environments that require unique modes of employment; equipment; and tactics, techniques, and procedures. A special operation is characterized as having one or more of the following traits: time sensitivity, high degree of risk, low visibility, cultural expertise, or collaboration with indigenous forces.[1] How is a force protected in a denied area, where the inherent risk is already increased? In other words, what does protection look like in an irregular warfare environment?

Background

Since 2016, 1st Special Forces Command has supported deployment requirements for a special operations joint task force, conducting mission command and supporting special operations at the two-star level. This support has included a mission readiness exercise and several large-scale Army exercises. In the absence of a formally established protection cell in the 1st Special Forces Command headquarters, the military police security force assistance team has provided personnel (including a protection chief) to fill the role of a protection cell during these exercises.

Protection Cell

For the exercises, the 1st Special Forces Command headquarters served as the special operations joint task force (SOJTF) headquarters with multiple subordinate commands from the combined SOJTF sent to Operational Detachment Alpha (ODA) echelons. Each exercise took place in the crisis domain, with the force countering a peer threat with equal or greater capabilities across the five domains (cyber, space, air, ground, and sea). The protection cell was assigned to the SOJTF staff and was responsible for all force protection requirements within the SOJTF. Given the assignment to a staff with minimal organic protection assets, coordination with organizations in all directions was paramount to ensuring and validating that adequate force protection measures were being implemented and adjusted as threats changed. The protection cell responsibilities stretched from the SOJTF headquarters in the rear area to the 12-man ODA in the close and deep areas and included all lines of communication and critical assets in between.

For the exercises, the prevalent risks were electronic-signature exploitation, operational security, and partner nation force survivability. The protection cell identified the biggest challenge in protecting electronic-signature and information security. Aside from minimizing the overall signature of the SOJTF, the primary concern was protecting the electronic signature emanating from the SOJTF to the subordinate units operating in denied areas as well as all linkages in between. Overcoming the effect of enemy jamming capabilities while maintaining sufficient protection required significant effort from cyber, space, and signal personnel in the protection working group. Additionally, electronic linkages from units to Family members at home were also of concern.

What resources are available for protection cells to visualize the current electronic signatures of their units? As capabilities continue to advance, cyber network defense plans are critical, but the development of tools and techniques that are more preventive than responsive is even more valuable. The protection cell proposed several ways to mitigate the enemy's ability to detect and exploit friendly electronic signatures. First, increased fortification around the command nodes physically impedes any electronic signature. Second, and most effectively, the protection cell explored and executed options to displace signatures through military deception.

The continuous publication of updated, specific, and deliverable operation security guidance prior to deployment and throughout operations was an effective operational security awareness and reinforcement tool for the protection cell. The protection cell delivered operational security guidance via annexes to operation orders, daily fragmentary orders, threat briefings, and smart cards—all delivered over secure communications before, during, and after the exercises. A key component of the operational security guidance consisted of enforcing and validating a communication plan using primary, alternate, contingency, and emergency (PACE) methods. Creating a PACE plan that is layered in protection at each level is a protection task that requires that public affairs, cyber, and signal personnel be included in the protection working group. Whereas conventional forces can enforce a no-cellular-phone policy and maintain operational communication, special operations forces units of action rely on commercial communication methods. Education on Android©, Apple©, Signal©, WhatsApp©, and other application security features can ensure that units avoid drawing attention to their specific location or to the location of the people—primarily indigenous persons—with whom they are communicating. The protection cell continued to be

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:

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

[2]Ibid.

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:

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

[2]Ibid.

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

[4]ADP 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.