Protection

Professional Bulletin

2023 Annual Issue

HEADQUARTERS, DEPARTMENT OF THE ARMY
Approved for public release; distribution is unlimited.
PB 37-23-1

U.S. Army
Maneuver Support Center of Excellence

Commanding General
MG Christopher G. Beck **573-563-6166**
<christopher.g.beck.mil@army.mil>

FIELDED FORCE INTEGRATION DIRECTORATE (FFID)

Director, FFID
COL Kevin W. Siebold **573-563-4148**
<kevin.w.siebold.mil@army.mil>

Deputy Director, FFID
Mr. Stuart D. Saulpaugh **573-563-5558**
<stuart.d.saulpaugh.civ@army.mil>

Chief, TRADOC Proponent Office–Protection, FFID
COL Joseph E. Elsner **573-563-7264**
<joseph.e.elsner2.mil@army.mil>

Deputy Chief, TRADOC Proponent Office–Protection, FFID
Mr. Barrett K. Parker **573-563-7105**
<barrett.k.parker.civ@army.mil>

CAPABILITIES DEVELOPMENT and INTEGRATION DIRECTORATE (CDID)

Director, Maneuver Support–CDID
COL Kenneth J. Frey **573-563-7158**
<kenneth.j.frey.mil@army.mil>

Deputy Director, Maneuver Support–CDID
Mr. Damon M. Yourchisin **573-563-8193**
<damon.m.yourchisin.civ@army.mil>

Chief, Maneuver Support Battle Laboratory
LTC Adam D. Akers **573-563-7259**
<adam.d.akers2.mil@army.mil>

Chief, Requirements Determination Division, Maneuver Support–CDID
Mr. Michael J. Martori **573-563-1201**
<michael.j.martori.civ@army.mil>

Deputy Chief, Concepts Division, Maneuver Support–CDID
Mr. Greg A. Dent **573-563-7955**
<gregory.a.dent2.civ@army.mil>

HOMELAND DEFENSE/CIVIL SUPPORT OFFICE

Director
Mr. David A. Engbrecht
<david.a.engbrecht.civ@army.mil> **573-563-2911**

Chief, Force Modernization Divison
Mr. Brian J. Boston **573-563-7679**
<brian.j.boston.civ@army.mil>

Protection is an official U.S. Army professional bulletin that contains information about the role of protection, the protection warfighting function, the Army Protection Program, and integration of protection capabilities to support the range of military operations. The objectives of *Protection* are to inform and motivate, increase knowledge, improve performance, and provide a forum for the exchange of ideas. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other U.S. Army publications.

Articles to be considered for publication are due 15 August. Send submissions by e-mail to <usarmy.leonardwood.mscoe.mbx.protectpb@army.mil>. Due to the limited space per issue, we normally do not publish articles that have already been published elsewhere. The U.S. Army Maneuver Support Center of Excellence reserves the right to edit material.

All photographs are official U.S. Army photographs unless otherwise noted. *Protection* is published exclusively online. It is available at the following links:

- <https://www.dvidshub.net/publication>
- <https://home.army.mil/wood/index.php/contact/publications/ppb>

DIGITAL SUBSCRIPTIONS are available at <https://www.dvidshub.net/publication>

Articles may be republished if credit is given to *Protection* and its authors.

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, Acting United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2323703

DOCTRINE DIVISION, FFID

Chief, Doctrine Division
Mr. Doug M. Loggins **573-563-4074**
<douglas.m.loggins.civ@army.mil>

Managing Editor
Ms. Diana K. Dean **571-588-0865**
<diana.k.dean.civ@army.mil>

Editor
Ms. Cheryl A. Nygaard **571-588-0884**
<cheryl.a.nygaard.civ@army.mil>

Graphic Designer
Mr. Dennis L. Schellingberger **571-588-0895**
<dennis.l.schellingberger.civ@army.mil>

Protection
Professional Bulletin
PB 37-23-1, 2023 Annual Issue

Maneuver Support Center of Excellence and Fort Leonard Wood Commanding General

Major General Christopher G. Beck

I am honored to have been in command at the U.S. Army Maneuver Support Center of Excellence (MSCoE), Fort Leonard Wood, Missouri, for 6 months, and I am proud to serve with this incredible team of professionals!

One of my responsibilities is to fulfill Army force modernization doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) requirements. Proponent requirements for Protection are designated in Army Regulation (AR) 5-22, *The Army Force Modernization Proponent System*.[1] As MSCoE leads the development and synchronization of Protection capabilities, we are all responsible! As we work together, let's stay mindful of our purpose—to be ready to fight and win our Nation's wars. Everything we do should contribute to a more lethal and cohesive force.

Your efforts in fiscal year (FY) 2023 were incredible, ensuring that, in 2030, Protection will be a continuous process that is assessed throughout operations and across the battlefield to deny the enemy freedom of action; enable access to friendly forces; and preserve our critical capabilities, assets, and activities. I am particularly excited about three efforts to better educate the force:

- Updating Army Doctrine Publication (ADP) 3-37, *Protection*.[2]
- Transitioning the Protection Integrator's Course from a pilot to a programmed institutional course in FY 25.
- Enhancing professional military education, including electives at the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas, and the U.S. Army War College, Carlisle, Pennsylvania, and improving assessments of captain's career courses.

In addition to these efforts, we will continue to explore Protection-related force design efforts for 2030 capabilities with guidance from the U.S. Army Combined Arms Center, Fort Leavenworth, and the U.S. Army Futures Command (AFC), Austin, Texas.

I am also very proud of AFC and the Maneuver Support–Capabilities Development and Integration Directorate in looking to 2040, including the recent completion of the all-domain Protection capabilities-based assessment gap analysis phase. With the resulting approved list of Protection capability gaps, we will begin FY 24 experimentation and workshops at Fort Leonard Wood to develop recommended approaches to materiel and nonmateriel solutions to apply the Protection warfighting function at echelons.

As we develop solutions, we ask for your continued support and input, including your participation in experiments, workshops, and recurring forums such as the semiannual Protection Working Group (institutional team engagement) and the Protection Warfighter Forum (operational force engagement). Based on your input in FY 23, we learned that there has not always been a consistent understanding of Protection. We listened and are now addressing your feedback by—

- Engaging leaders, including leaders at combat training centers and mission command training programs, to ensure that we help operational forces succeed.
- Ensuring the proper presence at warfighter exercises to better inform division and corps commanders of available capabilities.
- Assessing Protection in professional military education—from captain's career courses to electives at the Command and General Staff College and the U.S. Army War College—to ensure that we accurately inform and educate the next generation.
- Integrating Protection into the operations and targeting processes.
- Updating publications to better frame and clarify the following aspects of Protection in order to help commanders and staffs focus the right resources to enable mission success:
    - Foundational—concentrated on the Protection of individuals, units, platforms, or information.
    - Operational—focused on corps/division Protection cells and commanders.
    - Institutional—driven by policy, as dictated by AR 525-2, *The Army Protection Program*.[3]

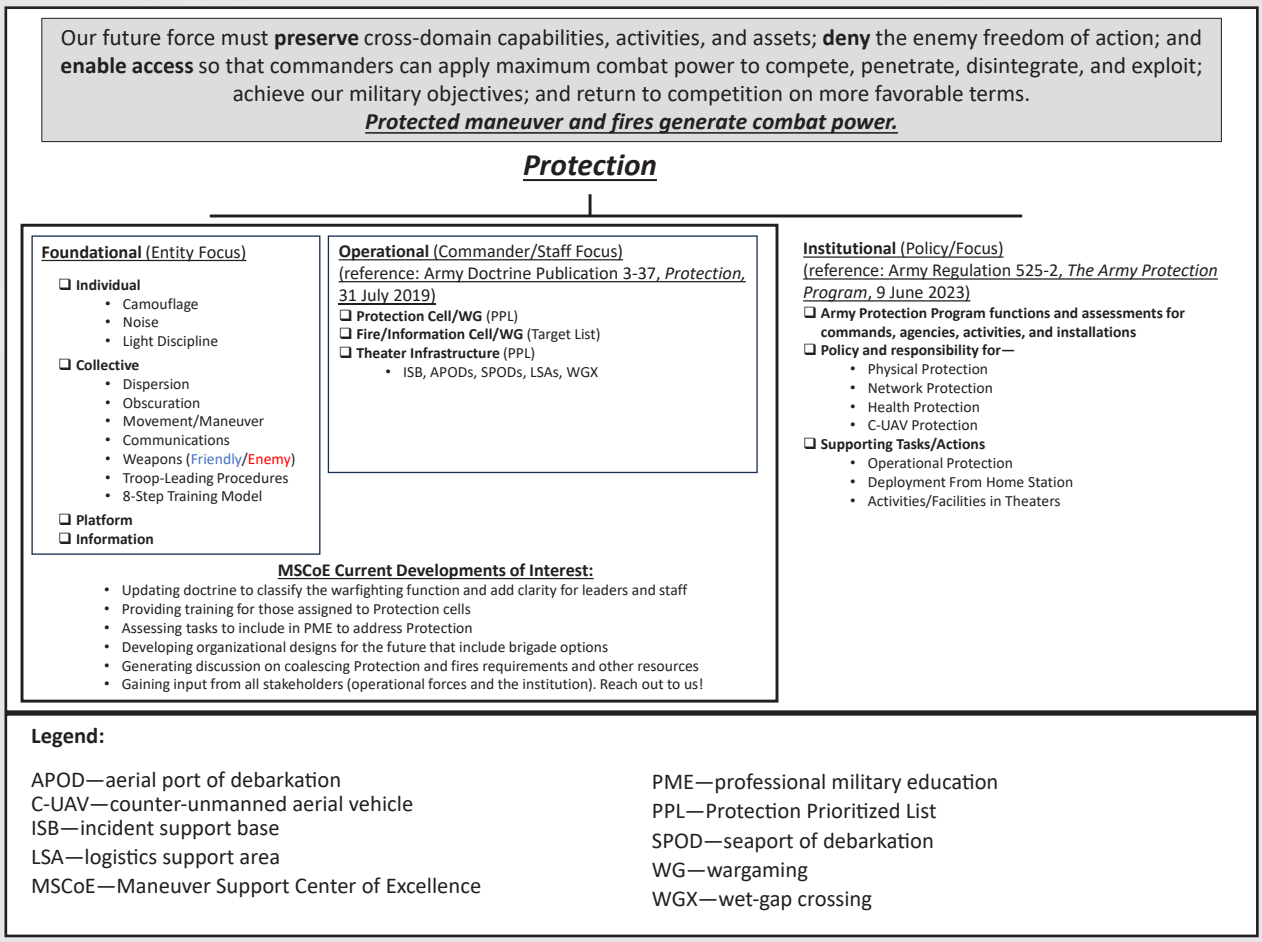


Figure 1. Protection

Although development and synchronization efforts span all aspects of Protection, MSCoE focuses on operational Protection, which synchronizes multidomain effects to create convergence at multiple decisive points.

As we develop and synchronize the Protection capabilities that our Army needs to fight and win today, in 2030, in 2040, and beyond, I see tremendous opportunity for continued progress in this great community of practice. Thank you for all you do!

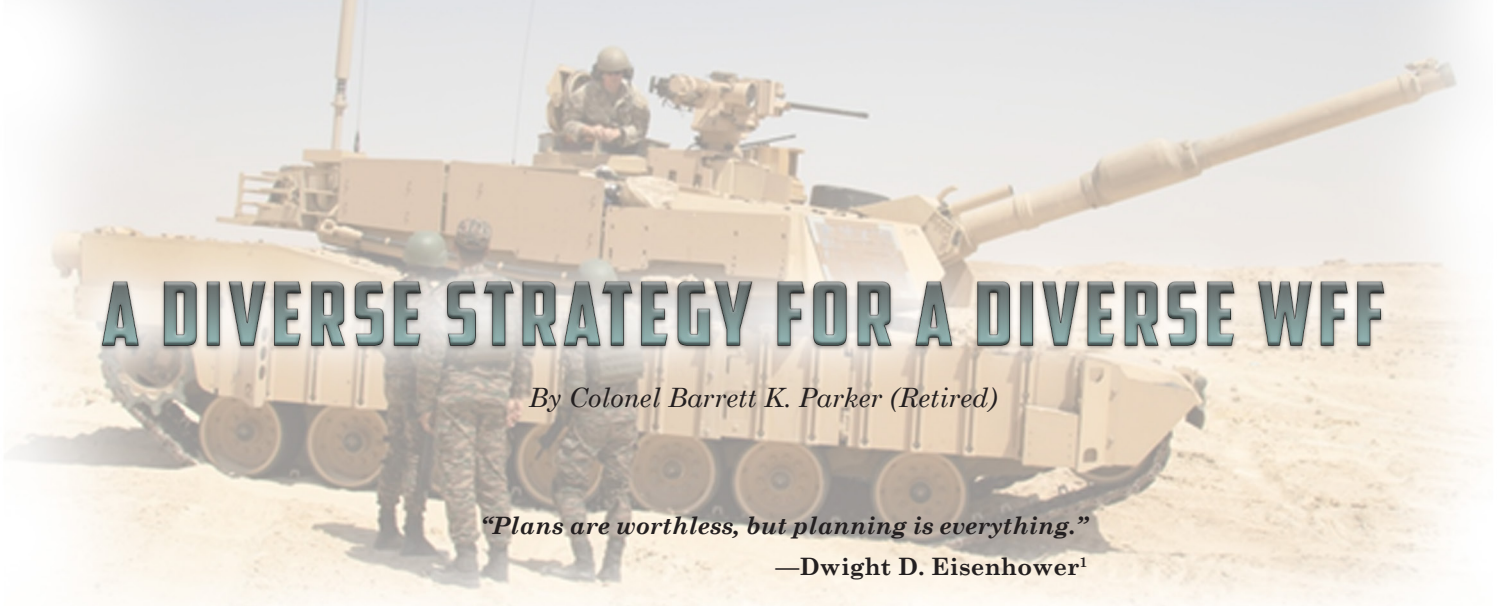
Victory Starts Here! Victory Through Skill!

Endnotes:

[1]AR 5-22, *The Army Force Modernization Proponent System*, 13 June 2023.

[2]ADP 3-37, *Protection*, 31 July 2019.

[3]AR 525-2, *The Army Protection Program*, 9 June 2023.



A DIVERSE STRATEGY FOR A DIVERSE WFF

By Colonel Barrett K. Parker (Retired)

"Plans are worthless, but planning is everything."

—Dwight D. Eisenhower[1]

According to the U.S. Army Training and Doctrine Command (TRADOC), "Army 2030 represents the largest force modernization and enterprise transformation in 40 years."[2] To keep pace, the U.S. Army Maneuver Support Center of Excellence (MSCoE), Fort Leonard Wood, Missouri, has embarked on creating a draft Army protection warfighting function (WFF) strategy designed to improve and evolve the protection WFF.

Through the years, the Army has produced very successful strategies. The "Big Five" procurement strategy,[3] which resulted in the delivery of the M1 Abrams battle tank, is one such success story. These strategies share a common theme; they first focus on a limited number of high-impact capabilities, deliverables, or qualities (such as a new battle tank or new field artillery with increased range) and *then* develop the family of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) solutions around the key deliverable.

Today's branch, regimental, and functional strategies typically follow a similar path, first focusing on a single high-visibility, high-impact capability or deliverable and then subsequently building around the deliverable by including other supporting DOTMLPF-P solution sets. Following this formula allows for the straightforward determination of improvement in terms of measures of performance/effectiveness. For example, if we want to increase the range of a weapon, then simple mathematics will show us how much more area could be engaged in comparison to that of the previous weapon system. Through basic threat analysis, we could ascertain how to best use this capability against current and future threat systems. From this, we could devise a strategy to optimize our advantage through changes in doctrine, updates to organization design, modifications in tasks and training, and enhancements to leader development.

"Improving by 1 percent isn't particularly notable—sometimes it isn't even noticeable—but it can be far more meaningful, especially in the long run. The difference a tiny improvement can make over time is astounding. Here's how the math works out: If you can get 1 percent better each day for a year, you'll end up 37 times better by the time you're done."[5]

Now, back to discussing the development of the draft Army Protection Strategy. Unlike other WFFs, the protection WFF consists of a highly diverse portfolio of capabilities. Maintained by 12 proponents, the 16 primary tasks of the protection WFF represent a marked departure from the traditional WFF construct. Obtaining and realizing any significant improvement to the protection WFF through the acquisition of a single DOTMLPF-P deliverable is impossible. Further, establishing measures of performance/effectiveness for protection WFF improvements is difficult since many protection challenges are unique to combat operations and very dificult to replicate. Several protection WFF primary tasks, such as personnel recovery, pose unique situations in which the value of new equipment or processes is often expressed subjectively.

Some regiments have already championed systems that provide protection against single hazards. For example, protection against chemical agents would be addressed in the U.S. Army Chemical, Biological, Radiological, and Nuclear School strategy. Therefore, an entirely unique approach to developing the overarching Army Protection Strategy is not just well advised, it's imperative.

The draft Army Protection Strategy must focus on our capability to reliably deliver the ability to provide comprehensive schemes of protection. To create "windows of protection," we must make the "preserve-deny-enable" vision of protection described in U. S. Army Futures Command (AFC) Pamphlet (Pam) 71-20-7, *Army Futures Command Concept for Protection 2028,*[4] a reality. The draft Army Protection Strategy must collectively address protection at all echelons (from Soldier to theater) across all components and plan solutions with the flexibility necessary to address new, unidentified threats generated by an adaptive adversary. The only way to accomplish this is to commit to a sports strategy known as "aggregation of marginal gains."

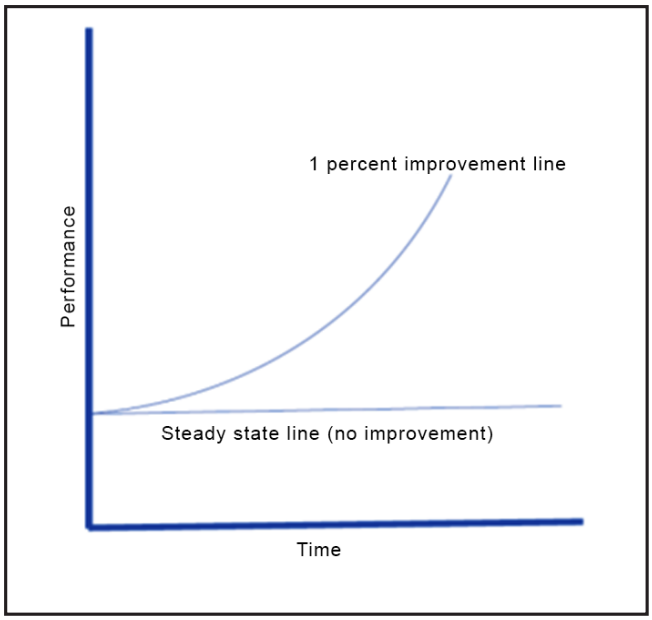


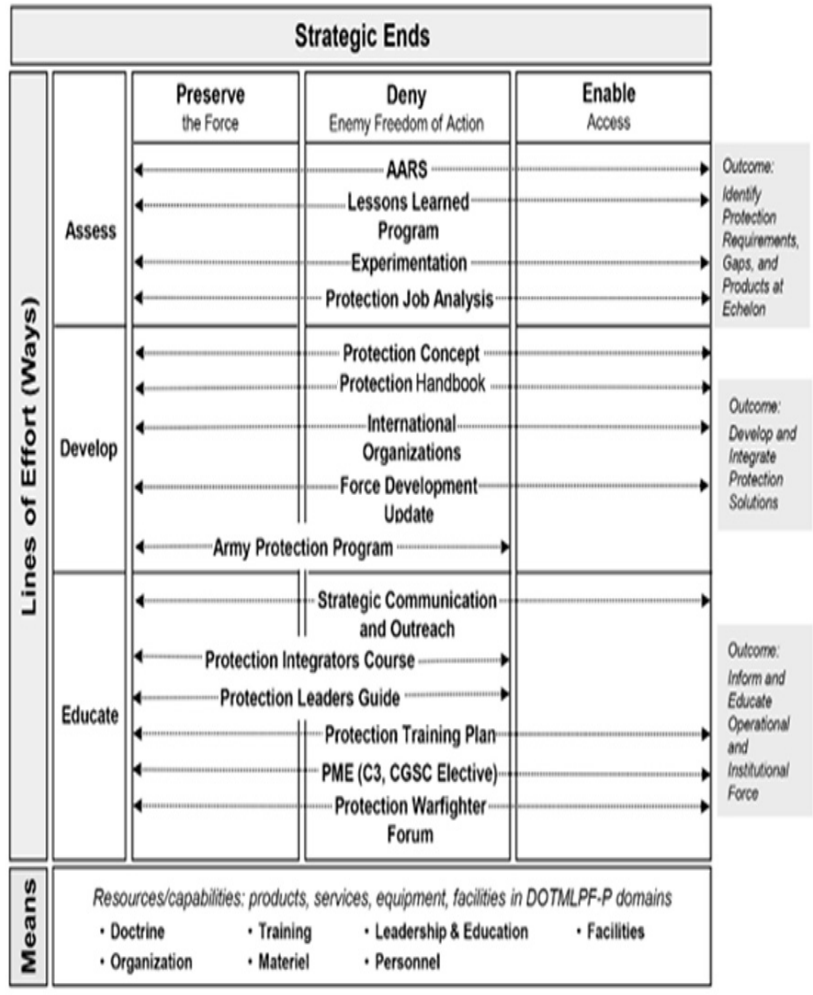
Figure 1. A daily 1 percent improvement will result in an overall performance improvement by more than 37 times by the end of the year.[5]

Mr. Dave Brailsford, performance director of a British cycling team, has described aggregation of marginal gains as the ". . . idea that if you broke down everything you could think of that goes into riding a bike, then improved it by 1 percent, you will get a significant increase when you put them all together; James Clear presents this philosophy and expounds upon it by stating that "Improving by 1 percent isn't particulary notable–sometimes it isn't even noticeable–but it can be far more meaningful, especially in the long run. The difference a tiny improvement can make over time is astounding. Here's how the math works out: If you can get 1 percent better each day for a year, you'll end up 37 times better by the time you're done."[5] Understanding this concept is essential for improving a complex portfolio such as the protection WFF, which is especially hard to evaluate with traditional metrics.

The draft Army Protection Strategy takes advantage of the aggregation of marginal gains concept by identifying dozens of individual DOTMLPF-P solutions that can be used to improve the protection WFF, addressing validated protection needs identified by AFC Pam 71-20-7 and subsequent work and then harmonizing and integrating those efforts.

For example, an examination of the leader development domain for protection reveals more than a dozen unique, ongoing efforts across the Army to improve the protection WFF. Current and projected solutions in that domain include conducting semiannual global Microsoft© Army 365 Teams-based protection WFF forums with all echelons-above-brigade protection cells; running quarterly Teams-based protection WFF working groups with all 12 TRADOC protection-owning proponents and dozens of other protection stakeholders; conducting podcasts in which changes in the protection WFF are discussed; maintaining ProtectionNet (the collaborative work forum for the protection community), located on milSuite at <https://www.milsuite.mil/community/spaces/apf/protectionnet>; conducting an annual protection conference; and creating a dynamic protection display for other conferences across the Army. Each of these leader development domain solutions interlock with solutions resident in other DOTMLPF-P domains, such as training development and protection lessons learned presented during protection WFF forums or protection engagement opportunities briefed during the Protection portion of the Army War College Theater Army Staff Course. Individually, none of these solutions "moves the needle"

(Continued on page 8)



Legend:
AAR—after action review
C3—captain's career course
CGSC—Command and General Staff College
DOTMLPF—doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
PME—professional military education

Figure 2. Army Protection Strategy ends, ways and means

PROTECTION INTEGRATION IN AN ARMORED CORPS: INSIGHTS FROM WFX 23–04

By Lieutenant Colonel Judd K. Young

In the 5th Century B.C., Sun Tzu wrote, ". . . the clever combatant imposes his will on the enemy but does not allow the enemy's will imposed on him."[1] The technological advancements that now enable unprecedented lethality during large-scale combat operations make his statement even more relevant today. Recently revised Field Manual (FM) 3-0, *Operations*, not only introduces multidomain operations as the new U.S. Army operating concept but also redefines the protection warfighting function as ". . . related tasks, systems, and methods that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action."[2]

The first multinational warfighter exercise (WFX) following the publication of FM 3-0 was rotation 23-04, conducted at Fort Cavazos, Texas, 18–27 April 2023, in which III Armored Corps (III AC) fought as a tactical-level multinational corps. Throughout the operations process, III AC sought to integrate a multifunctional, all-hazard concept of protection that leveraged active/offensive operations to deny enemy opportunities while more passive/defensive operations mitigated the remaining effects to protect critical capabilities and enable freedom of action.

Organizing

Unmanned aerial systems, loitering munitions, and long-range precision fires used against command posts (CPs) in Nagorno-Karabakh, Armenia, and Eastern Ukraine changed not only the character of war,[3] but also the way that units must array their command-and-control nodes, logistics, and critical assets. In preparation for WFX 23-04, III AC deliberately abandoned the traditional tent-based, three-node CP concept (consisting of tactical, main, and rear command post [RCP] nodes), opting for a more agile and survivable design capable of being hidden in plain sight, thereby reducing visibility and exposure across the electromagnetic spectrum.[4] The experimental concept involved the dispersal of the CP across four nodes based primarily on function. Whereas three nodes (RCP, current operations, and future operations) were positioned inside the area of operations, long-range planning, analysis, and assessments were conducted via reach-back to a fourth node placed in relative sanctuary.

Led by the III AC Deputy Commanding General for Support, the RCP node was comprised of elements of the III AC staff, the 13th Armored Corps Sustainment Command, and maneuver enhancement brigade staff. The RCP node synchronized protection and sustainment operations throughout the corps area of operations and exercised command and control for all units operating within the corps rear area. Organized as a "fighting CP," the RCP node was capable of handling the responsibilities of a unit assigned an area of operations (as outlined in FM 3-0) but relied on the maneuver enhancement brigade staff and mission command information systems to control airspace, clear fires, and perform command and control of area security tasks.

Operating predominately from the RCP node, the III AC Protection Cell coordinated full-spectrum protection operations across the depth of the corps area of operations. The nodal command and control construct resulted in the dispersal of protection staff across three of the four CP nodes. Although deliberate talent management decisions placed personnel where they could exert the greatest influence, manning constraints prevented the staff from operating at capacity across all nodes. The Protection Cell focused its efforts on conceptual planning in support of targeting, maneuver, and sustainment operations by synchronizing protection resources 72–96 hours prior to operations, while relying heavily on the associated functional brigades (maneuver enhancement; military police; engineer; chemical, biological, radiological, and nuclear; air defense artillery; and civil affairs) to conduct the detailed planning via bottom-up refinement.

Planning

The III AC staff diligently worked to understand the situation from the enemy perspective. The commanding general coached staff members toward "picking up the red pen first," which enabled them to visualize the enemy's capability, intent, targeting priorities, and pending decision points. A clear understanding of the enemy's delivery methods and high-pay-off target list enabled the targeting of specific systems in order to deny the enemy the opportunity to strike and allowed the III AC Protection Cell to effectively prioritize critical assets (belonging not only to III AC but also to others in the area of operations, including the combined forces land component command, allied forces, and the host nation) and align appropriate protection assets to mitigate the residual risk. Protection Prioritized Lists (PPLs) were developed for each phase of the corps order and refined by key events. The initial PPL was further refined through corps engineer brigade modeling that depicted the operational and humanitarian impacts of a potential "black swan"[5] attack on host nation infrastructure (such as those now occurring in the Ukraine/Russia conflict[6]).

Specific protection planning guidance emphasized aggressive area security operations, dispersion, survivability, camouflage, decoys, concealment, and electronic signature management. Deliberately targeting special-purpose forces at echelon not only disrupted enemy long-range fires but also denied the enemy the ability to take direct action against critical assets arrayed in the close and rear areas. To protect logistics, the 13th Armored Corps Sustainment Command dispersed sustainment nodes across small, tailorable, mobile support packages inside "position areas for sustainment." Modeled after the "position areas for artillery" addressed in field artillery doctrine, position areas for sustainment enabled frequent survivability moves within a designated area and mitigated risks posed by enemy observation and long-range fires. Nesting the priority of engineer effort with the PPL, the corps engineer brigade allocated dig assets to improve critical asset survivability behind the published corps engineer work line.[7]

The III AC Commanding General specifically directed that ". . . the corps must 'spring-load' to maximize operational reach," positioning sustainment assets "almost uncomfortably" far forward, moving rear boundaries as soon as possible, and continuously consolidating gains.[8] According to the *Military Review* article "Three Perspectives on Consolidating Gains," ". . . successful consolidation of gains ultimately denies the enemy the time, space, and psychological breathing space to reorganize for continued resistance."[9] And although the current version of FM 3-0 rescinds the term "consolidation area,"[10] III AC anticipated a complex hybrid threat and deliberately task-organized the RCP node with the organic mobility, antiarmor, and indirect-fire capabilities required to defeat bypassed conventional forces (up to a Level III threat) as far forward as possible, deny enemy special-purpose forces freedom of action, and neutralize meaningful resistance in the rear area.

Preparing

Prior to commencing operations, III AC conducted a corps level protection rehearsal with its subordinate divisions and enabling brigades. Conducted using the same terrain model used for three prior rehearsals (combined arms, intelligence collection/fires, and sustainment rehearsals), the protection rehearsal synchronized protection efforts that supported the overall schemes of maneuver and sustainment. Using the "box method,"[11] protection planners and III AC subordinate units rehearsed critical events such as the forward passage of lines, wet-gap crossings, and rear-boundary shifts. The protection rehearsal enabled a shared understanding of the anticipated enemy actions, to-scale weapons engagement ranges, positions of assets on the corps PPL, subordinate schemes of protection, and terrain management challenges associated with each critical event. The protection rehearsal stimulated updates to the rear area terrain management plan, prompted candid discussions regarding boundary shifts, and managed expectations regarding the positioning of air and missile defense (AMD) assets.

Executing

The fluid nature of large-scale combat operations requires an agile concept of protection, well-defined transition criteria, and clearly delegated decision-making authorities. Rapidly expanding lines of communication followed by unexpected delays with frequent transitions from offense to hasty defense quickly rendered the initial synchronization matrix obsolete. During WFX 23-04, the Coalition Forces Land Component Command task-organized an air defense artillery brigade in direct support of III AC, which enabled the commander of the 32d Army Air and Missile Defense Command to synchronize theater AMD operations while supporting the mission of the main effort[12]; however, repositioning AMD assets in a timely manner initially proved challenging. After being delegated authority to reposition AMD assets, the III AC Deputy Commanding General for Support approved templated moves in advance under clearly articulated security conditions agreed upon by the 32d Army Air and Missile Defense Command and III AC. He also discussed AMD moves with his division counterparts on a daily basis; and once they reported that the stipulated conditions had been met, movement began almost immediately.

Leveraging mission command information systems, air defense officers and junior noncommissioned officers readily enabled III AC to counter unmanned aerial systems and ballistic missiles. Although protection professionals often use the Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) Method[13] to assess risk to critical assets, the III AC targeting team was indirectly reminded that the CARVER Method was actually developed as a targeting technique.[14] By shifting focus to less-recuperable parts of the system, III AC targeteers enjoyed significantly more success in the counter-unmanned aerial systems fight.

Assessing

A deliberate protection working group (PWG) is essential for the assessment of current operations and mitigation of risk across all planning horizons. Although battle rhythms in large-scale combat operations are unrelenting, an effective PWG must be sequenced along the critical path so that its outputs directly feed the targeting cycle in a timely manner. Initially, III AC PWG assessed the previous 24 hours, conducted a systematic review of each PPL (synchronized by each air tasking order) over the next 72–96 hours, and identified the risks and the resources required to mitigate those risks. Over time, the PWG evolved to feed the corps assessment working group by evaluating protection-related transition criteria for the current and subsequent phases of the operation. The PWG served as a forum to ensure that bridging and boundary shifts remained on track. Once nested with the joint movement board process, the PWG not only synchronized security operations for critical resupply but also identified opportunities to emplace additional line-of-communication bridging to open lateral routes and shorten division lines of communication by more than 100 kilometers.

Conclusion

Given a determined enemy with persistent intelligence, surveillance, and reconnaissance, coupled with effective electronic warfare capabilities and massed long-range fires, the protection warfighting function is more relevant than

ever. Tasks intended to "prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action"[15] require an inherent combined arms approach and an offensive mindset throughout the operations process.

Endnotes:

[1]Sun Tzu, *The Art of War*, 5th Century B.C., with translation and commentary by Lionel Giles, Capstone Publishing, 2022.

[2]FM 3-0, *Operations*, 1 October 2022.

[3]Matthew R. Bigelow, "Protection and the Change in the Character of War," *Protection* 2022 Annual Issue.

[4]Sean C. Bernabe, "Observations from Warfighter Exercise 23-04: A Multinational Corps as a Tactical Headquarters in Large-Scale Combat Operations," Strategic Landpower Symposium, 11 May 2023.

[5]A "black swan" is defined as "a highly improbable event that is unpredictable, carries a massive impact and, after the fact, appears less random, and more predictable." (Nassim N. Taleb, *The Black Swan: The Impact of the Highly Improbable,* Random House, 2007.)

[6]Dan Peleschuk, "Evidence Grows of Explosion at Collapsed Ukraine Dam," Reuters, 9 June 2023, < https://www.reuters.com/world/europe/ukraine-security-service-says-it-intercepted-call-proving-russia-destroyed-2023-06-09>, accessed on 12 October 2023.

[7]FM 1-02.1, *Operational Terms*, 9 March 2021.

[8]Bernabe.

[9]Michael Lundy et al., "Three Perspectives on Consolidating Gains," *Military Review*, September–October 2019.

[10]FM 3-0.

[11]"The box method is based on a critical event in which a detailed analysis of a critical area is completed, such as an engagement area, a wet-gap crossing site, or a landing zone. It works best in a time-constrained environment, such as a hasty attack, and is particularly useful when planning operations in noncontiguous areas of operation. When using this method, the staff isolates the area and focuses on critical events." (U.S. Army Combined Arms Center [CALL] Handbook 19-18, *Commander and Staff Guide to Rehearsals: A No-Fail Approach*, July 2019.)

[12]Glen A. Henke, "Once More Unto the Breach: Air Defense Artillery Support to Maneuver Forces in Large-Scale Combat Operations," *Military Review*, March–April 2023.

[13]FM 1-02.1

[14]Christopher Schnaubelt et al., *Vulnerability Assessment Pocket Guide: A Tool for Center of Gravity Analysis*; RAND Corporation, 2014.

[15]FM 3-0.

Lieutenant Colonel Young is the deputy commanding officer for the 89th Military Police Brigade, Fort Cavazos, Texas. During WFX 23-04, he served as the protection chief for III AC. He holds a bachelor's degree in wildlife management from Frostburg State University and a master's degree in business and organizational security management from Webster University.

("A Diverse Strategy for a Diverse WFF," continued from page 5)

much; but collectively, and over time, significant improvement is realized.

The Army Protection Strategy will be organized along three main lines of effort: assess, develop, and educate. Primary processes will be associated with each of those lines. Individual DOTMLPF-P solutions (the means) will be subsequently identified and developed, leading to a significant number of unique solutions—all interlocked and supporting a defined outcome as well as the larger strategy.

As the Army and the joint force move toward large-scale combat operations, Army protection tactics, techniques, and procedures; programs; and systems must keep pace. By committing to a strategic approach of aggregation of marginal gains for the protection WFF, MSCoE will deliver the diverse and resilient program of steady protection improvement needed to support the Army division of 2030.

Endnotes:

[1]Dwight D. Eisenhower, "Remarks at the National Defense Executive Reserve Conference," 14 November 1957, *The American Presidency Project*, <https://www.presidency.ucsb.edu/documents/remarks-the-national-defense-executive-reserve-conference>, accessed on 11 October 2023.

[2]"How the Army 2030 Division Fights," TRADOC Proponent Office–Echelons Above Brigade, August 2023.

[3]The "Big Five" was a collection of procurement programs "designed to reestablish the technological supremacy of U.S. land forces and reinvigorate conventional capabilities in the Vietnam War; it included the Apache AH-64 helicopter, UH-60 Black Hawk helicopter, M1 Abrams battle tank, Bradley fighting vehicle, and MIM-104 Patriot missile system (Robert Farley, "What if the Army's 'Big Five' Weapons Program Had Failed?" *The National Interest*, 24 July 2020, <https://nationalinterest.org/blog/reboot/hat-if-us-armys-big-five-weapons-programs-had-failed-165555>, accessed on 11 October 2023).

[4]AFC Pam 71-20-7, *Army Futures Command Concept for Protection 2028*, 9 April 2021.

[5]James Clear, *Atomic Habits: An Easy & Proven Way to Build Good Habits & Break Bad Ones*, Random House Business, London, 2018, pp. 13–14.

Colonel Parker (Retired) is the deputy chief of the TRADOC Proponent Office–Protection, Fielded Force Integration Directorate, MSCoE. He holds a bachelor's degree in earth science from Pennsylvania State University, University Park; a master's degree in environmental management from Samford University, Homewood, Alabama; a master's degree in engineering management from Missouri University of Science and Technology at Rolla; and a master's degree in strategic studies from the U.S. Army War College, Carlisle, Pennsylvania. He retired as a colonel from the U.S. Army Reserve.

ADP 3-37, *Protection*: An Update to the WFF

By Captain Carlos J. Valencia

As we shift our focus to large-scale combat operations against peer adversaries, it is more important than ever that we understand the enemy threat, the operational environment, and all forms of contact in order to protect essential military personnel, equipment, infrastructure, and data. In recent years, protection has gained more notoriety as the technologies of the future have become the threats and hazards of today.[1] Predicting, mitigating, and protecting against enemy threats and hazards remain essential for Army forces to generate combat power at home stations through the Army Protection Program during competition below armed conflict to set conditions for crises and armed conflict. Once crises and armed conflict begin, a transition from the Army Protection Program to the protection warfighting function (WFF) occurs, allowing commanders to protect their forces and preserve their freedom of action on the battlefield. Protection of Army forces, equipment, and installations stems from many factors, such as regulations, programs, standard operating procedures, tactical operations, and the protection capabilities and systems employed to protect a force; still, dedicated planning is arguably the most critical factor. Protection planning and contributions to the operations process are continuous and enduring endeavors that we undertake as we adapt to and predict the actions of our enemy (see Figure 1). Through a comprehensive, integrated, layered, and redundant approach, protection planning can mitigate garrison risk and afford commanders the time, forces, and ability to impose their will on the battlefield. As with previous versions of Army Doctrine Publication (ADP) 3-37, *Protection*,[2] the pending 2023 revision will provide guidance on the protection WFF and establish the doctrinal foundation for commanders and staffs who are responsible for planning, preparing, executing, and assessing protection in support of Army operations.

The October 2022 publishing of the capstone Field Manual (FM) 3-0, *Operations*,[3] changed the Army operational concept to multidomain operations. Doctrine writers and developers routinely review early drafts of capstone publications to aid in ensuring concurrency with subject matter areas, and FM 3-0 was no exception. Because all other doctrine must nest with FM 3-0, its impending publication set off a massive effort to begin revisions of the doctrinal libraries governed

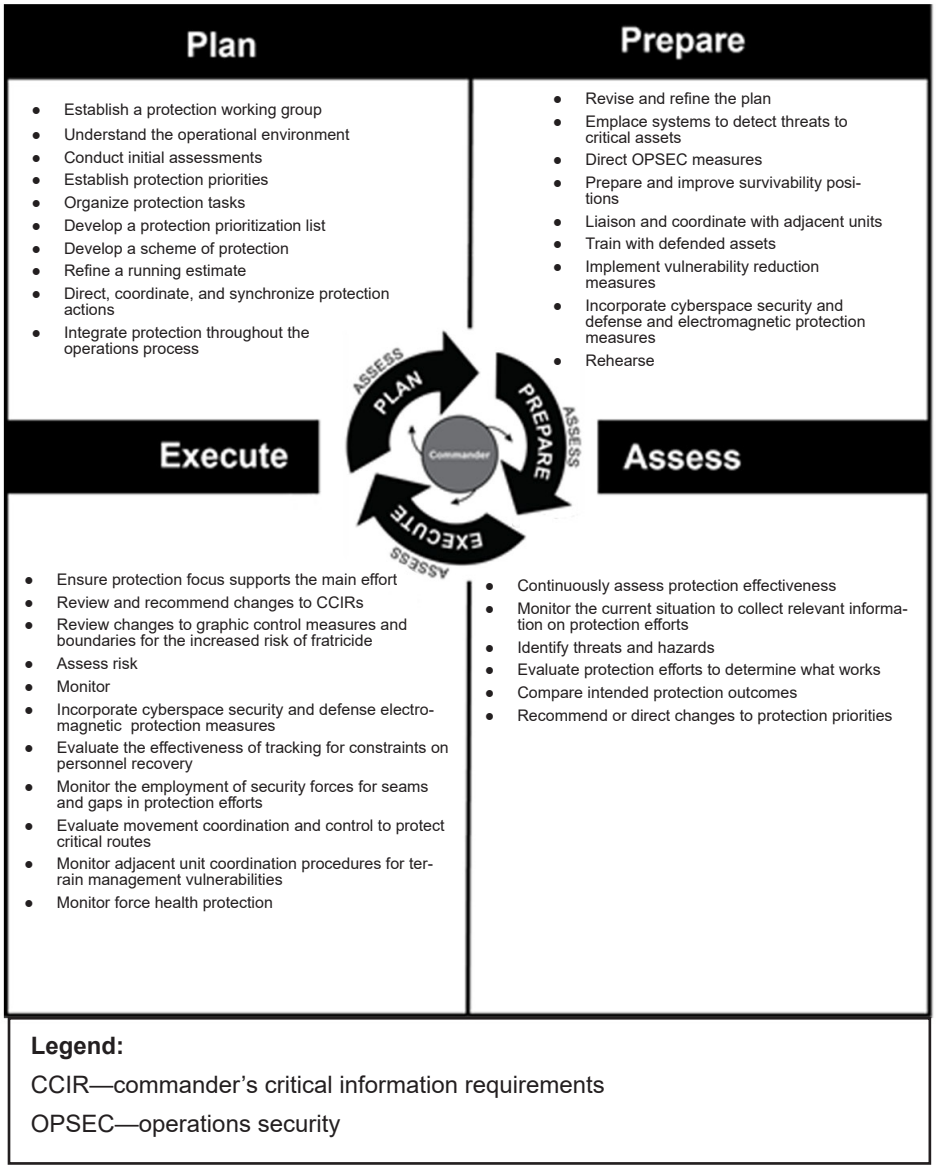


Figure 1. Integration of protection throughout the operations process

by each center of excellence. Starting in February 2022, after providing assistance with the development of FM 3-0, the Doctrine Division, Fielded Force Integration Directorate, Maneuver Support Center of Excellence (MSCoE), Fort Leonard Wood, Missouri, began the doctrine development process on ADP 3-37. Following five working group meetings comprised of stakeholders from 12 organizations, two 60-day staffing periods (for the initial and final drafts), and 1,440 comments from the force, the 2023 revision of ADP 3-37 is now nearly ready for publication.

The 2023 ADP 3-37 revision will be consistent with previous protection WFF doctrine. The same 16 primary tasks will be retained; however, these tasks will be grouped into four categories—conduct risk management, protect capabilities, protect areas, and protect information—to provide a better understanding of their organization and employment (see Figure 2).

A significant change has been made to the definition of the protection WFF itself though. The protection WFF was previously defined in ADP 3-0, *Operations,* as "the related tasks and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission."[4] Many believed that this definition fell short of the true importance of the WFF, as it limited most protection preconceptions and planning efforts to survivability. During the development of FM 3-0, MSCoE doctrine developers suggested an updated definition that would better support multidomain operations. As introduced in the latest revision of FM 3-0, the protection WFF is now defined as "the related tasks, systems, and methods that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action."[5] This new definition expands our understanding of the protection WFF, particularly by acknowledging that protection consists of more than survivability and passive actions, and includes stopping threats and hazards before they occur. Most importantly, the new definition acknowledges the critical role that the protection WFF plays in preserving a commander's ability to have freedom of action to exploit opportunities at each echelon and through the depth of the operational environment and strategic situation. This new definition was vital in developing the 2023 revision of ADP 3-37.

Conduct risk management. Risk management is the process used to identify, assess, and control risks and make decisions that balance the cost of risk with the benefits of mission. It focuses on the mission and the force.

Protect capabilities. Capabilities protection involves measures taken to prevent or mitigate friendly detection or the impact of enemy action and to intercept or destroy threats and hazards before they can inflict damage to Army capabilities. Elements of capability protection include—

- Survivability. (Protect against detection and lethal fires.)
- Air and missile defense. (Protect against air and missile threats.)
- CBRN operations. (Protect against contamination.)
- Force health protection. (Protect against threats and hazards to health.)
- Electromagnetic protection. (Protect against electromagnetic spectrum threats.)
- Physical security. (Protect personnel, resources, and information.)
- Personnel recovery. (Protect isolated personnel.)

Protect areas. Protecting areas prevents, mitigates, and disrupts the enemy's ability to gain positions of advantage; maintain freedom of action; destroy friendly critical capabilities, assets, and activities; and influence third-party actors, surrogates, proxies, and irregular criminal threats across the operational environment, including force projection and generation platforms in the homeland and abroad. Area protection includes —

- Area security. (Secure areas, lines of communication, and critical assets from threats.)
- Antiterrorism. (Personnel, property, and resources.)
- EOD. (Protect against explosive hazards.)
- Police operations. (Protect forces, populations, critical infrastructure, and assets and enable stability [Rule of Law].)
- Detention operations. (Protect against detained persons.)
- Populace and resources control. (Protect people and their economic resources.)

Protect information. Protecting information requires enduring measures that protect and defend friendly information and information systems. These measures are designed to conceal information from, and deny information to, the threat; protect information from unauthorized modification; protect information from unauthorized destruction; and enable information advantage. Information protection includes —

- OPSEC. (Protect critical information and indicators of friendly force actions.)
- Cyberspace security and defense. (Protect cyberspace.)

Legend:

CBRN—chemical, biological, radiological, and nuclear OPSEC—operations security

EOD—explosive ordnance disposal

Figure 2. Protection categories

Additionally, the following updates or expansions will be included in the 2023 revision of ADP 3-37:

- Protection challenges make commanders and staffs think about unique obstacles that they must be prepared to overcome in support of Army operations during competition below armed conflict, crisis, and armed conflict.
- The protection WFF manifests itself differently at each echelon and across the operational framework (see Figure 3) and during competition below armed conflict, crisis, and armed conflict.
- Commanders and staffs synchronize operations and tasks from other WFFs that complement and reinforce protection, such as—
  - Conduct security operations.
  - Conduct countermobility operations.
  - Perform tactical deception.
  - Provide intelligence support to protection.
  - Combat fratricide.
  - Perform general engineering.
  - Perform security measures.
  - Counter explosive hazards.
  - Collect forensic and biometric material.
  - Conduct Army space operations.
- Protection capabilities are integrated throughout the operations process, and commanders and staffs use the operations process to determine protection requirements and priorities and to direct, coordinate, and synchronize protection efforts and capabilities across all domains to reduce risk, mitigate identified vulnerabilities, and create windows of opportunity to achieve mission success.
- Roles and responsibilities of the protection cell at corps, echelon, and below are identified; sections that make up the protection cell are described; the relationship of the protection cell to other key staff sections is explained; and the working groups in which the protection cell must participate are identified.

Protection is vital to protecting critical capabilities, preserving combat power, and mitigating risk across all domains, dimensions, and strategic contexts. The new version of ADP 3-37 will remind leaders that protection is not limited to a specific domain or branch of the Army but applies to the Army as a whole. All units must take it upon themselves to

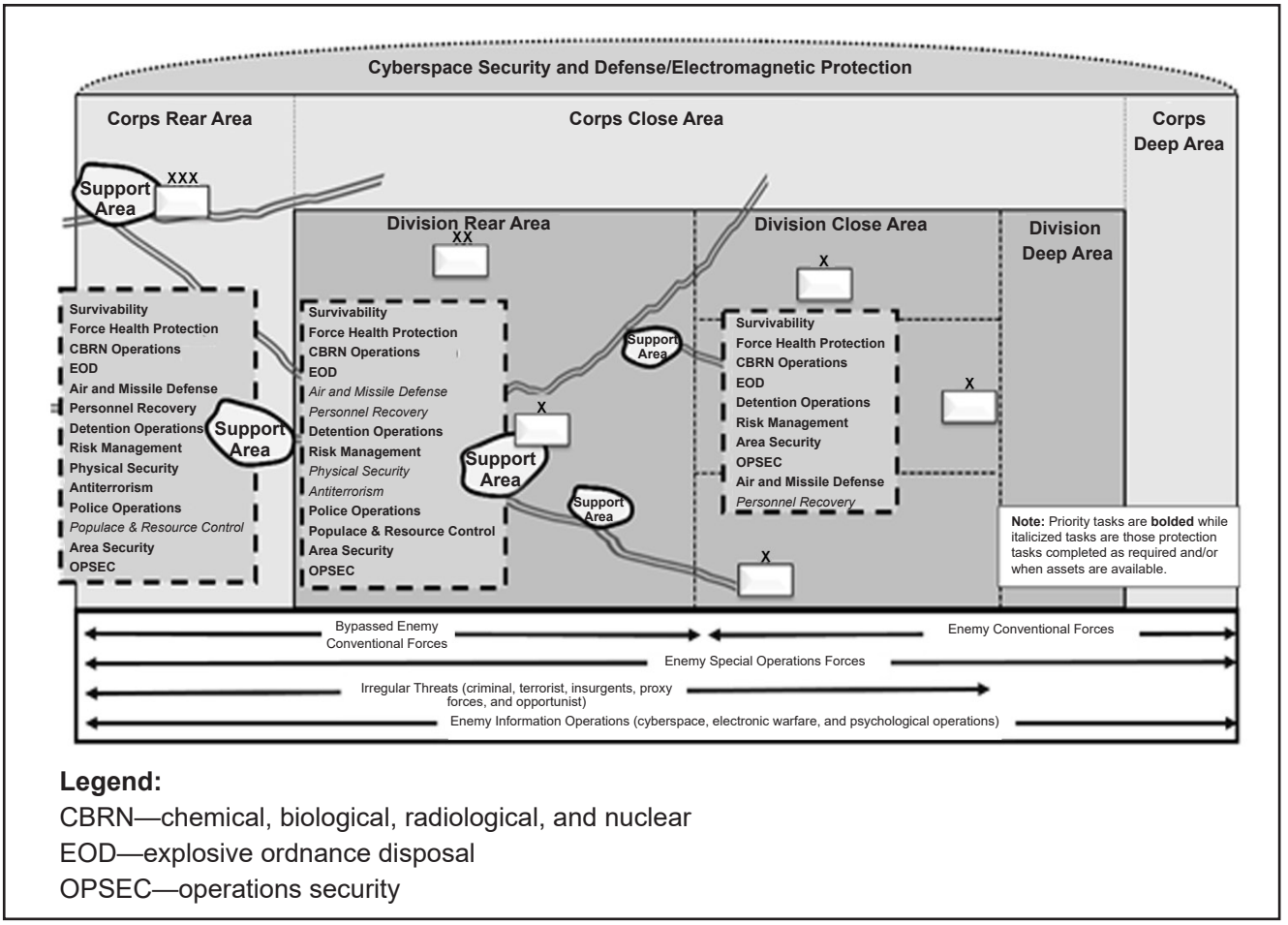


Figure 3. Protection considerations within a corps area of operations during large-scale combat operations.

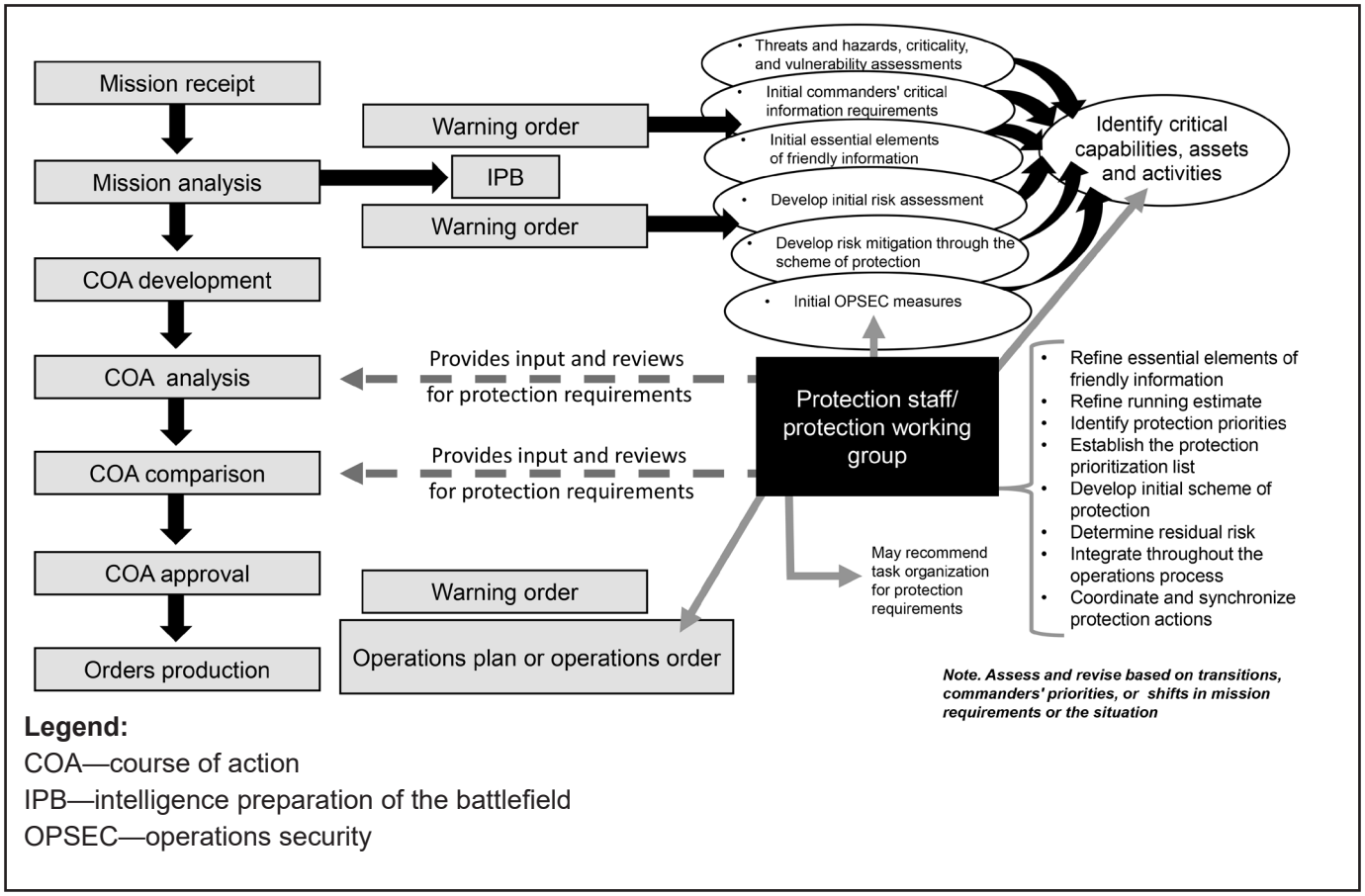


Figure 4. Protection planning

employ security operations, modify the tempo, take evasive action, maneuver to gain positional advantages, decrease electromagnetic signatures, and disperse forces to improve survivability in order to have the combat power necessary to achieve mission success. These survivability tasks fundamentally start with each Soldier achieving proficiency in his or her everyday Soldier tasks and fieldcraft. Additionally, ADP 3-37 will implore protection staffs to be forward-thinking, to predict threats and hazards that may not be readily apparent, and to integrate these predictions and planning efforts into the operations process (see Figure 4). Protection leaders must understand their place within a staff and not only serve as subject matter experts in their field but also become protection WFF experts, which can only be done by gaining an understanding of ADP 3-37.

ADP 3-37 will build on the collective knowledge and wisdom we've gained during recent operations, numerous lessons learned, and doctrinal revisions throughout the Army. ADP 3-37 nests with ADP 3-0; FM 3-0; FM 3-90, *Tactics*;[6] and other recently revised doctrine and emerging publications and is rooted in time-tested principles and fundamentals while also accommodating new technologies and organizational changes.

Once published, be sure to download a copy of ADP 3-37 from <www.armypubs.army.mil> or obtain a copy from your unit publication manager.

Endnotes:

[1]Joint Publication (JP) 3-0, *Joint Operations*, 18 June 2022.

[2]ADP 3-37, *Protection*, 31 July 2019.

[3]FM 3-0, *Operations*, 12 October 2022.

[4]ADP 3-0, *Operations*, 31 July 2019.

[5]FM 3-0.

[6]FM 3-90, *Tactics*, 1 May 2023.

Captain Valencia is a doctrine analyst/writer for the Military Police Doctrine Branch, Doctrine Division, Fielded Force Integration Directorate, MSCoE. He holds a bachelor's degree in history from the University of Texas, San Antonio.

PROTECTION ANALYSIS

By Mrs. Sonia L. Taylor

The primary purpose of Army analysis is to provide the information that senior leaders need to make informed decisions or better understand complex problems. Over the years, protection has been one of those complex problems that the Army has struggled to adequately analyze and understand. Numerous studies and experiments have been conducted on topics including force protection, base defense, decision tools, sensors, and systems to examine portions of protection; however, there has been no holistic study of protection with full community involvement until now.

As the Army focuses on modernizing and shaping the future force, a new view of protection—one that promotes moving the Army to be more proactive in all domains—has led to the development of U. S. Army Futures Command (AFC) Pamphlet (Pam) 71-20-7, *Army Futures Command Concept for Protection 2028*,[1] also known as "the Protection Concept." Shortly after the Protection Concept was signed in April 2021, the Maneuver Support (MS) Capability Development Integration Directorate (CDID), Fort Leonard Wood, Missouri, was tasked to lead a multiyear capability-based assessment (CBA) for all-domain protection (ADP) so that AFC could assign priority gaps to organizations to work on doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) integrated solutions. The ADP CBA, which began in Fiscal Year (FY) 2022, was challenged with translating the Protection Concept into something that the Army could do.

The Protection Concept describes how the Army realizes ADP using protection activities and requirements spanning multiple proponents and organizations to achieve required effects on the expanded battlefield when properly integrated and synchronized at echelon across the competition continuum. Multidomain operations pose challenges that will require the future force to proactively deny and defend against enemy action and conduct protection activities to achieve the three core components of the Protection Concept:

- Preserve critical capabilities, assets, and activities.
- Deny threats and enemy freedom of action.
- Enable access to achieve protected windows of superiority.

The CBA—one of the primary analysis tools used to study Army concepts and capabilities—provides the analytic foundation for developing joint capabilities integration and development system documentation. It is a structured study that helps capability developers identify requirements and associated capability gaps to determine future warfighting requirements and recommend potential materiel or nonmateriel approaches to resolving or mitigating those gaps.

The ADP CBA process consists of three phases:

- Needs analysis—identifying required capabilities and their associated operational characteristics and attributes.
- Gap analysis—determining the capability gaps and associated operational risks.
- Solutions analysis—assessing possible solution approaches for the capability shortfalls.

The problem statement, or study issue, for the ADP CBA is "How can the Army converge effects to identify, open, and exploit protected windows of superiority while maintaining persistent protection for select mission-essential nodes, thus realizing ADP for multidomain operations?"

The methodology, or approach, for conducting the ADP CBA begins with the Protection Concept, moves through the three CBA phases, and ends with recommendations and solutions. To help alleviate conflicts of interest and strive to conduct an unbiased assessment, a retired general officer has been serving as a senior mentor to guide the discussion and challenge conventional thinking. Oversight is provided by a study advisory group comprised of the CDID directors and chaired by the U.S. Army Combined Arms Center Deputy to the Commanding General. To date, the ADP CBA has completed the needs analysis and gap analysis phases. The analytic conditions for both phases consisted of a series of workshops that brought the protection stakeholders together to facilitate discussions and data collection. Approximately 115 participants from more than 30 organizations provided thorough examination and lively debate and offered many insights concerning the protection of the future force in a complex multidomain environment.

The needs analysis phase aimed to determine what must be accomplished and what capabilities the warfighter needs to achieve mission success within an operational context. Four vignettes within an approved scenario were designed using the multidomain operations context of competition, armed conflict, and return to competition (as described in the Protection Concept)—with an extra phase called "crisis deter aggression" added between competition and armed conflict. It was not feasible to chase all 44 required capabilities defined in the Protection Concept within the constraints of the CBA, so the focus was narrowed to 12 that directly supported the problem statement. Participants were challenged to think more broadly in their approach to protection. As discussions unfolded, the scope expanded to include other appropriate tasks from any required capabilities detailed in the Protection Concept. As the tasks were reviewed to determine which were directly related to the required capabilities, they were grouped into four areas: new tasks, tasks

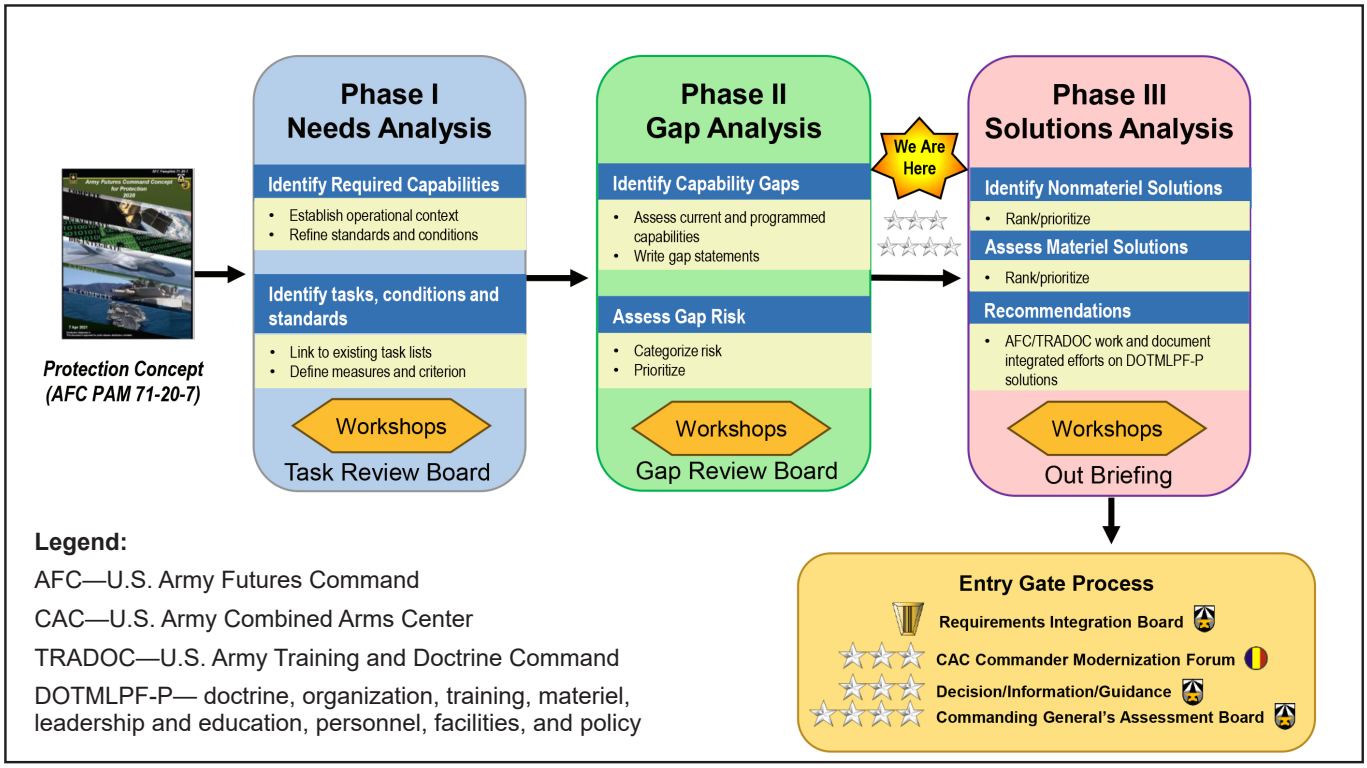


Figure 1. Capability-based assessment process and assessment approach

of interest to all warfighting functions, tasks of interest to two or more warfighting functions, and critical tasks per vignette. The needs analysis resulted in the identification of more than 150 total tasks, of which more than 20 were new. Following the task review board, the study advisory group approved the required capabilities and tasks, enabling the transition to gap analysis.

During the gap analysis phase of the ADP CBA, which was conducted in FY 23, the tasks, measures, and metrics were further refined to determine the tasks that failed, the resulting gaps, and the operational risk to mission accomplishment if the gaps were not mitigated. At the recommendation of senior leaders, the first gap analysis workshop focused on the operational- to theater strategic-level tasks and the second workshop focused on division and below tactical-level tasks. Once the failed tasks were identified, stakeholders developed gap statements and assigned an operational risk category of extremely high, high, moderate, or low to each gap. After a presentation to the gap review board and a review by the study advisory group, the final gap analysis product consisted of a prioritized list of gaps. Overall, there were more than 60 extremely-high-risk and more than 20 high-risk gaps for Army 2030 formations in the given scenario, which involved a 2035 threat and operating environment.

The ADP CBA solutions analysis phase, which is designed to assess potential DOTMLPF-P approaches to solving the prioritized capability gaps approved during the gap analysis phase, is poised to be completed in FY 24. Protection stakeholders have identified numerous tasks, metrics, and gaps in order to find possible solutions to realize ADP. AFC will assign examination of materiel and organization gaps to the CDIDs, and the U.S. Army Training and Doctrine Command (TRADOC) will assign examination of the doctrine, training, leadership and education, personnel, facilities, and policy gaps to the centers of excellence during solutions analysis. Both commands will synchronize efforts to ensure the delivery of integrated solutions.

The ADP CBA is not just an MS-CDID or AFC effort but a whole Army effort that touches all CDIDs, proponents, and stakeholders within the Army Modernization Enterprise. Analysis has produced many key takeaways, enabling leaders to stretch conventional thinking, apply new approaches, and integrate efforts. Protection is not a traditional warfighting function; it is a mindset that everyone must develop in order for the Army to succeed on the future battlefield. Operationalizing protection and fully realizing the concepts of AFC Pam 71-20-7 depend on the results of the ADP CBA in developing new protection solutions and educating the force.

Endnote:

[1]AFC Pam 71-20-7, *Army Futures Command Concept for Protection 2028*, 9 April 2021.

Mrs. Taylor is an operations research/systems analyst serving as the deputy director of the Maneuver Support Battle Laboratory, Fort Leonard Wood. She holds a bachelor's degree in mathematics from Harding University, Searcy, Arkansas.

What is Protection in 2040?

By Mr. Michael J. Martori

"The protection warfighting function is essential to preserving future capabilities in multidomain operations."

—D. Scott McKean[1]

Protection has always been a complicated and complex warfighting function—from the War on Terrorism (when protection was defined by base defense, barriers, physical security, persistent ground surveillance, and blimps, which are inherently passive and reactive) to today's need for dispersion, sensor-to-shooter interactions, and robotics, which shift the focus to active measures that provide overmatch. If you ask 10 different people what they think protection is, you will likely get 10 different answers. So, what is protection?

As the Army modernizes through its signature systems and adaptive formations, leaders and Soldiers must understand protection in 2030 and, more importantly, operationalized protection. Approving U.S. Army Futures Command (AFC) Pamphlet (Pam) 71-20-7, *Army Futures Command Concept for Protection 2028*,[2] in 2021 was a significant first step in realizing these goals. Fast forward to today; and now, it is AFC's mission to deliver the Army of 2030 and design the Army of 2040. Protection in 2030 must include ways to preserve critical capabilities, assets, and activities against threats in all domains; deny the enemy freedom of action; and enable access so that commanders can apply maximum combat power to defeat the enemy. Protection capabilities must deny, degrade, and disrupt enemy positions of advantage, freedom of action, and abilities to destroy friendly critical capabilities, assets, and activities across the operational environment, including the homeland.

In speaking about the ever-changing character of warfare, General James E. Rainey, AFC Commanding General, makes these three points:[3]

- There is a paradigm shift from "conducting fires to maneuver" to "conducting maneuver to fire." Some of you may be shaking your heads, but think about our future fight and how fires will shape that fight—even more than troops on the ground will. General Rainey says, "I personally think fires is going to move back up ahead of maneuver to the top slot. We're going to maneuver to place fires versus using fires to condition maneuver."
- There is a need for capable formations that are enabled by human-machine integration. The Army fights by formation, and capable formations—with all the systems, personnel, and training necessary to fight and win our Nation's wars—are required. Through human-machine integration, robotic systems will become our forward line, or "first contact," if you will.
- We must "figure out" protection. It's this point that keeps me up at night. Hearing a senior Army leader say that we must "figure out protection" is scary. Large-scale combat operations are very different than operations conducted during the last fight. On a battlefield where you can be killed if you can be seen, and you can be seen; well . . . you fill in the blank. In that fight, protection is more critical than ever. Although artificial intelligence, machine learning, dispersion, deception, signature systems, and capable formations will all provide protection, more must be done.

For protection to truly be understood in 2040, commanders must change the way they think about it. Think about the last warfighter exercise in which you were involved and about the role of the protection cell in that exercise. How did the protection coordinator influence the fight—or even make him- or herself be heard, outside of providing the commander with a Protection Prioritized List (PPL)? Too often, protection personnel talk about protection with other protection personnel, which is mildly interesting but not very useful. The protection cell is responsible for preserving the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within the division operational

(Continued on page 18)

THE EOCOP AND ITS PLACE IN LSCO

By Captain Stephen M. Hartman

"Anyone can recognize a pattern; it's having the courage of your convictions to act on it that matters. Audacity isn't taking senseless risks or being rash; it's a natural by-product of confidence and knowledge . . .."

—Pete Blaber[1]

The Army is making a concerted effort to address challenges arising from large-scale combat operations (LSCO) conflicts. As tragic as the current conflict between Ukraine and Russia is, it has provided the United States and its allies with the opportunity to develop technology, training, and a force structure to better suit possible near-peer conflicts within all warfighting functions. One area of focus within the explosive ordnance disposal (EOD) community involves understanding where EOD battalion and group leaders can best support a maneuver commander's intent during LSCO.

An EOD technician participates in a 2-day Unmanned Aircraft System Threat Defense Course.

During counterinsurgency operations, EOD leaders at the 71st Ordnance Group, Fort Carson, Colorado, and their subordinate battalions proved to be invaluable through their ability to relay and map the evolution of enemy tactics, techniques, and procedures; provide expert analysis on improvised explosive device (IED) trends within a combined joint task force commander's area of operations; and ensure that EOD forces were equipped with nuanced EOD explosives, equipment, and tools inherent to the EOD mission. The IED challenges faced in the counterinsurgency fight made multiplicity of the EOD capability more important than ever. As IEDs have proven to be a formidable adversary to the greatest Army in the world, this looming threat will likely never cease to exist. Additionally, the complexity of IEDs would presumably evolve as technology evolves. Both points are evident in the Russian-Ukrainian conflict.

The importance of IEDs and like threats that have been notable in recent counterinsurgency conflicts can be diminished by the vast explosive, chemical, and sometimes nuclear threats that may occur during Phases II and III of a LSCO conflict. Maneuver commanders do not have the appetite to stop the pacing and tempo necessary to be competitive in a LSCO fight—and rightly so. EOD leaders and those within the protection warfighting function must discern ways to provide maneuver commanders with a greater ability to make informed decisions while also maintaining a productive offensive operation.

As divisions and corps train in decisive-action training environments, EOD battalions and groups simultaneously seek to integrate with their respective maneuver counterparts (EOD battalions aligned to a division, EOD groups aligned to a corps, and so on). These invaluable repetitions are essential in warfighter exercises, as they allow staff at all levels to synchronize warfighting functions to enable victory,

stress the importance of staff and staff functions, and most importantly, allow for innovation within warfighting functions and processes in preparation for LSCO with a near-pear threat. Of the innovations within the EOD community, implementation and evolution of the explosive ordnance common operating picture (EOCOP) have most benefited the commander's decision-making process in the decisive-action training environment.

In support of I Corps during Warfighter Exercise 23-1, the 71st EOD Group fully implemented the first iteration of EOCOP, utilizing a Command Post Computing Environment (CPCE) as the essential medium. Provided by the EOD commander, the ECOP portrays a myriad of explosive threats and exploitation opportunities. The EOCOP is scalable, as it highlights explosive hazards and explosive-based considerations from the company to corps levels. Utilizing the CPCE and other battle-tracking mechanisms, EOD commanders can articulate explosive threats, which, without the EOCOP, would be unbeknownst to a commander. Unlike an obstacle overlay, the EOCOP illustrates unexploded ordnance saturation zones (which become inadvertent minefields) resulting from high rates of enemy and friendly fires. These saturation areas can potentially slow and canalize movement due to the presence of scattered munitions, which may include large amounts of high explosives and/or armor-piercing technologies. The EOCOP also tracks locations/discoveries of high-priority weapon caches/ammunition supply points and possible weapon technical intelligence locations/discoveries. The EOCOP has the incredible potential to inform commanders, influence their decision points, and provide the insight necessary to allow survivability of maneuver and logistics. With the EOCOP, EOD leaders provide value by recommending division and corps sustainment areas and identifying locations with greater explosive risks to forces, as well as pinpointing appropriate locations for consolidation of gains and preparation of a defense—all without running the risk of revealing a commander's maneuver tempo.

EOD technicians participate in a 2-day Unmanned Aircraft System Threat Defense Course. (U.S. Army photograph by Staff Sergeant Apolonia Gaspar)

While the EOCOP proved undeniably effective during its first actual implementation in an exercise environment, value could certainly be added. First, EOD missions and future operations could be reported through the CPCE, as that is the Army program of record. EOD technicians currently report all missions, demolition operations, technical intelligence discoveries, and many other actions through the Explosive Ordnance Disposal Information Management System. The issues with the current means of reporting are that it is stovepiped within the EOD community, as only EOD technicians may utilize the Explosive Ordnance Disposal Information Management System, and the information input into the system is not illustrated to enhance understanding of the battlespace regarding explosive hazards. Hybridizing EOD reporting requirements with the capabilities of the CPCE would allow for a better shared understanding of the battlespace, modernized EOD reporting, and increased efficiency within EOD formations. Additionally, using the CPCE

Teams ran full mission profiles during the 71st EOD Group maneuver support training. (U.S. Army photograph by Staff Sergeant Apolonia Gaspar)

to report EOD incidents would allow EOD teams on the ground to make reports to EOD leaders in real time. This repository of information could also be used to address and mitigate issues during the stabilization phase of the of the operation. A well-established and sustained EOCOP is imperative for successful joint communication and protection efforts within the area of operations. Enforcing a shared understanding of explosive hazards on the battlespace allows all agencies, departments, and branches of the military to benefit from a well-maintained and disseminated EOCOP. Second, and more importantly, integration with an artificial intelligence/machine-learning system is essential for EOD support for discerning explosive and explosive ordnance threats. The platform must be capable of searching for, and deriving meaningful information from, web-based sources such as various media outlets, social networks, news stories, uploaded videos, and video logs in order to gain an information advantage. The platform must then be able to identify, recognize, and distinguish explosive ordnance threats found during searches and logically categorize them on a map within the CPCE. Commanders who gain an informational advantage can quickly and accurately gain situational awareness, allow for informed and swift decision making, and exert influence in their areas of operations. Such capabilities would provide EOD battalions and groups with historical and real-time information and intelligence on unexploded ordnance; new explosive hazards or munitions requiring reporting and/or interrogation; and emerging adversary tactics, techniques, and procedures. With these capabilities, EOD leaders may present lifesaving recommendations to and for Soldiers on the ground and ensure that EOD technicians are better equipped to mitigate, attack, and exploit explosive threats with precision and veracity.

As the Army seeks to better understand roles and best practices within the LSCO paradigm, it is imperative that EOD professionals—as well as all other professionals within the Army—seek to evolve and prepare for the possibility of a LSCO fight. EOD personnel have a profound opportunity to assist commanders in making knowledgeable and audacious decisions to fight and win our Nation's wars.

Endnote:

[1]Pete Blaber, *The Mission, the Men, and Me: Lessons From a Former Delta Force Commander*, Dutton Caliber, New York, 2017, p. 234.

Captain Hartman is the commander of Headquarters, Headquarters Company, U.S. Army Garrison, Fort Carson, Colorado. He holds bachelor's degrees in biology and Christian studies from Crown College, St. Bonifacius, Minnesota.

("What is Protection . . . ," continued from page 15)

area. If the PPL were integrated as a product to synchronize operations for the next 72–96 hours—along with the air tasking order framework that fires personnel use to plan air support, indirect fires, and aviation attacks—into centralized planning, that would be useful! Integrating the PPL into the air tasking order cycle would allow for thorough staff analysis and coordination to maximize resources, while also enabling the commander to assess risk to the mission during decisive operations. Like the fire support coordinator who (with the targeting team) provides approved guidance, the high-payoff target list, the attack guidance matrix, and target selection standards in relationship to the intelligence and operations situation briefings, the protection coordinator provides guidance on resources needed to protect the approved PPL, assesses task force capabilities and the availability of resources, and then deconflicts future PPLs—all while coordinating resources for decisive operations 72–96 hours before an operation. Protection must be engrained in commanders' thought processes and integrated into the operations process.

If protection in 2040 resembles what it does today, our Army risks failure. Although opinions differ, most leaders can describe what protection currently looks like, what enables it, and what effects it has on mission success. If you ask those same leaders about those same three aspects of protection in 2040, I wonder if you would get any answer at all—never mind differing opinions.

In closing, I offer this description of protection in 2040: "Protection in 2040 will be fully integrated into the operations process through the commander's decision boards, enabled by machine learning and algorithms that fuse data and information to assist commanders in making informed, real-time, risk-based decisions and by systems supported by human-machine integration that provide protected maneuver to enable precision fires."

Endnotes:

[1]AFC Pam 71-20-7, *Army Futures Command Concept for Protection 2028*, 9 April 2021.

[2]Ibid.

[3]General James E. Rainey, Association of the United States Army Global Force Symposium and Exposition, Huntsville, Alabama, 28 March 2023.

Mr. Martori is the chief of the Requirements Determination Division, Maneuver Support–Capability Development Integration Directorate, Futures and Concept Center, AFC.

THE RUGGED BRIGADE AND DCRF 22:

PREPARING TO RESPOND TO CBRN DISASTERS

By Lieutenant Colonel Danielle Millien, Major Ben M. Cox, Captain Paul A. Kantner, and Captain Brent M. Stout

Relevance and History of Engineers

Engineers have always been the problem solvers of the battlefield, and the U.S. Army Engineer Branch remains the most diverse and versatile branch within the Department of Defense across the spectrum of military applications today—both in large-scale combat operations (LSCO) and defense support of civil authorities (DSCA) operations. Evidence of the impact of engineers on warfare can be found throughout history, dating to the beginning of war. From the defensive fortifications and watch towers of the Iron Age to the sophisticated Greek catapults of the 3d Century B.C. to the innovative Roman fortresses of the 5th Century A.D., the history and impact of military engineers can be realized wherever advances in fortifications, armament, or terrain-shaping technology and techniques are found. During 17th-Century siege warfare, the French famously employed sappers, or "trench diggers," who dug trenches toward and underneath besieged forts to explosively breach enemy positions. Essentially, military engineers have always answered the call to find and apply innovative solutions to the rising military challenges of the era.

Modern Engineer Versatility

In the modern U.S. Army, the versatile, problem-solving Engineer Branch is collectively comprised of almost 20 engineer military occupational specialties. Each specialty—including engineer divers, surveyors, firefighters, power production and distribution specialists, geospatial experts, electricians, plumbers, carpenters, masons, concrete and quarrying specialists, heavy-equipment operators, combat engineers, and numerous others—contributes to shaping the operational environment and addressing relevant challenges. Whether tasked to construct tactical obstacles, build infrastructure, repair airfields, destroy minefields, clear routes, or create maps, the specialty engineers enable the Engineer Branch to fill any job and tackle any task. The motto *Essayons*, translated from French as "Let Us Try," appropriately hints at the versatile application and inherently adaptable nature of the branch—both of which are necessary on the modern battlefield.

DCRF

One of today's challenging Army missions involves training, maintaining, and employing a joint, all-hazards, no-notice response force known as the defense chemical, biological, radiological, and nuclear response force (DCRF), which is one component of the Department of Defense chemical, biological, radiological, and nuclear response enterprise (CRE). It is composed of dedicated and allocated local, state, and federal forces that conduct emergency chemical, biological, radiological, and nuclear (CBRN) response operations to address CBRN incidents anywhere within the United States and its territories.

While probable response scenarios encompass chemical plant explosions or other emergencies potentially caused by large natural disasters such as hurricanes or wildfires, the most dangerous response scenario is one in which the detonation of a nuclear device occurs in a major metropolitan city. Ultimately, the DCRF aims to save lives and minimize human suffering. The DCRF mission resides on the DSCA end of the spectrum of military applications and, therefore, requires a thorough understanding of the legal implications of employing U.S. Code, Title 10, *Armed Forces*,[1] military forces within the continental United States. Training, maintaining, and employing a joint, all-hazards response force requires versatility and sufficient skill in a broad spectrum of specialties—not a narrow application of a niche skill set. It is no wonder that the Department of Defense continues to rely on U.S. Army engineer brigades to command and control the tactical elements of this consequential joint response force.

TF-OPS

The U.S. Army Forces Command annually tasks a Regular Army engineer brigade to a 2-year assignment with task force–operations (TF-OPS), the tactical core of the DCRF formation. DCRF falls under the U.S. Army Northern Command, which tasks a joint task force–civil support (JTF-CS) to command and control the entire DCRF force, including four brigade level task forces—TF-OPS, task force–logistics, task force–aviation, and task force–medical—and various other specialty

enablers that offer additional signal, human resources, legal, chemical, medical, and religious support capabilities. It is the responsibility of the TF-OPS commander and staff to synchronize task force movement in and around the response area; receive guidance from JTF-CS; liaise with the incident or area commander of the civilian emergency response infrastructure; and coordinate for logistics, aviation, and medical support from the other brigade task forces. The 2-year DCRF assignment in TF-OPS consists of equipping and training nearly 5,200 Soldiers during the first year, or "train-up year," and sustaining readiness in the second year, or "mission year (MY)." During the train-up year, participating units receive special equipment, conduct key leader conferences, participate in tabletop exercises, validate technical training, perform command post operations, execute internal staff exercises, and take part in leader development courses. During the MY, TF-OPS units receive a prepare-to-deploy order requiring them to be ready to deploy within 24 to 48 hours (depending on the force package to which the unit is assigned) of a no-notice disaster event. Units maintain readiness by participating in regular task force status update briefings and executing various joint sustainment exercises.

TF-OPS Headquarters and Formation

The TF-OPS formation includes three battalion task forces and five distinct enabler units. Each battalion task force, identical in purpose and capability, is led by an engineer, CBRN, or military police battalion. Each battalion includes a CBRN company, an area support medical company, a general-purpose force (GPF) company, and an urban search and rescue platoon. Each GPF may be comprised of either an engineer company or a military police company, and an engineer construction company usually fills the urban search and rescue requirement to search for and extract victims.

The TF-OPS enabler units are critical to the success of the overall DCRF mission; they comprise a joint force where the necessary specialized capabilities of the Army, U.S. Air Force, and U.S. Marines are consolidated under one command. Specifically, TF-OPS enablers include an Army engineer construction company, an Army mortuary affairs platoon, an Air Force radiation assessment team, and Air Force rapid engineer deployable heavy operational repair squadron engineers. The Marine chemical biological incident response force (CBIRF) is typically considered a separate task force (even though it is part of the consolidated command) due to its inherent ability to operate independently from the rest of the TF-OPS formation. For some of the units in the TF-OPS task organization (CBRN company or area support medical company), the assigned DCRF tasks align with their unit organic mission-essential task list. For others (battalion headquarters, the engineer or military police companies compromising the GPF, engineer construction company serving as the urban search and rescue platoon), the required DCRF tasks may bear little resemblance to the unit mission-essential task list.

A rescue team breaches and enters a confined space in search of victims. (Photograph by Marine Corps Staff Sergeant Jacqueline A. Clifford)

The battalion task forces must come together to provide six core capabilities, as outlined in the JTF-CS "OPLAN 3500-19 Overview":[2]

- Mission command and communications.
- CBRN identification and detection.
- Urban search and rescue.
- Mass casualty and noncasualty decontamination.
- Medical triage and stabilization.
- Air and ground evacuation.

The Rugged Brigade as Leader of DCRF 22

The Army Forces Command tasked Headquarters Company, 36th Engineer ("Rugged") Brigade, Fort Cavazos, Texas, as the TF-OPS unit for DCRF 22. In June 2021, the Rugged Brigade began receiving a series of in-briefings to start the DCRF 22 train-up year. From June 2021 to May 2022, the brigade conducted internal leader development classes, hosted mobile training team visits from JTF-CS, initiated regular touch points with the TF-OPS down trace battalions and companies, and executed a series of train-up exercises in preparation for a joint, multiechelon collective training validation exercise.

Before officially assuming the TF-OPS mission, DCRF units must validate their training in the Guardian Response exercise at the Muscatatuck Urban Training Center, Camp Atterbury, Indiana. The Muscatatuck Urban Training Center is home to top-tier urban training facilities that emulate

various realistic response scenarios, including a train crash, underground tunnel networks, a flooded neighborhood, a prison, a church, a hospital, and rubble piles; rubble roads containing hundreds of cars to be cleared by the TF-OPS engineer construction company enabler can also be created. Guardian Response is the only DCRF exercise that encompasses the entire JTF-CS formation, allowing units to test their response, mission systems, processes, and procedures. Using numerous contractors and role players, the Civil Support Training Activity, U.S. Army North, observes, coaches, trains, and validates units at Guardian Response. The Rugged Brigade took the opportunity to test inherited operating procedures and pave the way for new and enhanced response techniques and procedures for various aspects of the response force during its Guardian Response validation exercise in May of 2022.

The Rugged Brigade and MY 22

Once validated at Guardian Response, the Rugged Brigade officially assumed the DCRF mission and received the associated 24-hour prepare-to-deploy order. From 1 June 2022 to 31 May 2023, the Rugged Brigade led monthly status update briefings and regular task force activities. The brigade continued conducting leader development sessions regarding DCRF topics and maintained contact with higher, adjacent, and subordinate units. Mission planning conferences hosted by JTF-CS enabled mentoring relationships between the units that were on mission and those preparing to assume the mission. The conferences covered critical topics such as the deployment sequence; operation synchronization; and DCRF equipment use, storage, and handover planning factors. The conferences allowed face-to-face engagements of key leaders at the battalion, brigade, and division levels, ensuring adequate knowledge sharing and management between all pertinent stakeholders.

The 62d Engineer ("Hammer") Battalion, 36th Engineer Brigade, served as Battalion Task Force 1 for DCRF 22. During the annual recertification event "Determined Response," the Hammer Battalion developed new joint service tactics, techniques, and procedures by commanding and controlling an unprecedented relief operation between CBIRF and a battalion task force. The process included eight deliberate steps:

- Initial link-up.
- Operations overview and debriefing.
- Key leader terrain walk.
- New unit area occupation.
- New operator equipment familiarization.
- Gradual force integration.
- Process management handover.
- Operator exfiltration by the previous unit.

This type of operation is advantageous for scenarios in which the CBIRF establishes initial operations at a new response site and then reaches the point where it needs relief in order to maintain sufficient patient throughput. In preparation for the operation, the Hammer Battalion conducted multiple terrain model rehearsals with all stakeholders and refined tactical command procedures to include connections between the civilian incident commander and staff, the command team assigned to manage mass casualty decontamination operations, the CBIRF commander, the urban search and rescue teams, the GPF commander, and the medical treatment and evacuation commander. To command and control a complex and multifaceted formation, the Hammer Battalion tactical command post embedded a team of liaisons with each significant operation component. Occupying an operationally advantageous area, the battalion tactical command post could quickly receive and process information, track operational status through execution checklists, and report progress to higher echelons. With up to six liaisons employed at once, tactical-level feedback was rapid, enabling operational decision making to be flexible and effective.

A Marine scans a Soldier for notional radiation and chemical particulates during a simulated decontamination mission. (Photograph by Marine Corps Staff Sergeant Jacqueline A. Clifford)

Lessons Learned

The keys to Rugged Brigade success during DCRF 22 included the implication of a joint LSCO and DSCA training glide path, effective knowledge management, and consistent stakeholder engagement. TF-OPS units were faced with competing requirements and commanders with differing priorities. However, each one was still required to conduct DCRF training, validation, and sustainment activities.

The Rugged Brigade implemented a joint glide path in which Soldiers and leaders in LSCO and DSCA operations were simultaneously trained when possible, preparing for Warfighter 23-04 as the culminating LSCO training event while also staying ready to respond in support of DCRF DSCA operations. Incorporating clear training objectives for lines of effort maximizes the benefits of multiechelon collective training exercises. Planning efforts, communication across the formation, and the use of knowledge management systems are made more effective through the alignment of the correct human and material resources to the DCRF line of effort. Each unit undergoes heavy turnover during the 2-year DCRF assignment, but keeping the same trusted agents, liaisons, and lead planners where possible makes a substantial difference in mission success.

Soldiers assigned to the 172d CBRN Company and Marines assigned to the CBIRF prepare a simulated casualty for decontamination. (Photograph by Marine Corps Staff Sergeant Jacqueline A. Clifford)

Engineers Leading Joint Forces

Engineers have always been the problem solvers of the battlefield, and the Army Engineer Branch remains the most diverse and versatile branch within the Department of Defense across the spectrum of military applications. Evidence of the impact of engineers on warfare can be found throughout history and remains overtly significant where LSCO and DSCA operations are concerned. The Engineer Regiment will continue to answer the Nation's call, whether shaping the ever-changing operational environment on the modern battlefield or leading joint task forces in response to a disaster on the home front. The engineer Soldier has no choice but to fill any job, tackle any task, and continue singing *Essayons* in war and peace.

Essayons: **We serve America and the U.S. Army Corps of Engineers.**

Endnotes:

[1]U.S. Code, Title 10, *Armed Forces*.

[2]"OPLAN 3500-19 Overview," slide show, JTF-CS, 26 October 2021.

Lieutenant Colonel Millien is the commander of the 62d Engineer Battalion. She served as the DCRF Battalion Task Force 1 commander throughout DCRF 22. She holds a bachelor's degree in French from the U.S. Military Academy—West Point, New York, and a master's degree in organizational leadership from Norwich University, Northfield, Vermont. She is currently working toward an advanced degree in international relations from the London School of Economics. She is also a graduate of the U.S. Army Command and General Staff College.

Major Cox is the brigade operations officer (S-3) for the 36th Engineer Brigade. He served as the brigade plans chief during the DCRF 22 train-up year and as the battalion operations officer, 62d Engineer Battalion (DCRF Battalion Task Force 1) during DCRF MY 22. He holds a master's degree in geological engineering from the Missouri University of Science and Technology at Rolla. He is also a graduate of the U.S. Army Command and General Staff College.

Captain Kantner is the commander of Company B, CBIRF, Naval Support Facility, Indian Head, Maryland. He holds a bachelor's degree in communications from the University of Pittsburgh, Pennsylvania, and a master's degree in business administration from the Naval Postgraduate School. He is also a graduate of the U.S. Marine Corps Expeditionary Warfare School.

Captain Stout is the commander of the 104th Engineer Construction Company, 62d Engineer Battalion. He served as the lead planner, lead trusted agent, and lead liaison for the 36th Engineer Brigade (TF-OPS) during the 2022 DCRF train-up year and as the 62d Engineer Battalion (DCRF Battalion Task Force 1) plans chief during MY 2022. He holds a bachelor's degree in mechanical engineering from the U.S. Military Academy—West Point; a master's degree in engineering management from the Missouri University of Science and Technology at Rolla; and a graduate certificate in nuclear weapons effects, policy, and proliferation from the Air Force Institute of Technology.

OPERATIONALIZING RISK MANAGEMENT FOR DIVISIONS AND CORPS

By Lieutenant Colonel John Gervais (Retired) and Lieutenant Colonel Nathan E. Brookshire

According to Army Doctrine Publication (ADP) 6-0, *Mission Command: Command and Control of Army Forces,* risk is "the exposure of someone or something valued to danger, harm, or loss" and "because risk is part of every operation, it cannot be avoided."[1]

Commanding generals (CGs) must accept risk in order to reap the rewards of employing their combat power. However, they do not simply gamble with their division or corps. They have entire staffs that collect and refine information, allowing them to minimize risk to the mission as well as risk to the force. Division and corps staffs excel at determining how U.S. forces will engage and defeat the enemy. However, most staffs need to improve their ability to mitigate enemy effects on friendly combat power and the mission. This article presents a methodical approach to operationalizing risk management for division and corps level operations, which will provide CGs with improved visualization of risk in time and space, input for CGs' friendly forces information requirements (FFIR), and an edge to win at the decisive point.

The new approach to operational risk is based on the following tenets:

- It is challenging to apply the current accident-focused Army risk assessment model at higher-echelon large-scale combat operations (LSCO); a paradigm shift is required for better applicability to LSCO.
- Risk should be avoided, eliminated, and/or mitigated before the CG accepts residual risk. The warfighting functions (WFFs) are linked to these risk decision options.
- FFIR should be developed with the same rigor as priority intelligence requirements (PIRs).
- Risk management begins during mission analysis. Wargaming serves as the laboratory for testing risk reduction measures and should assist in developing decision points.
- Risk should be visually presented to the CG in time, space, and purpose, with linkage to FFIR to drive decisions.

Staffs discuss risk during each phase of the military decision-making process as well as during operations. However, risks must often be revised and better understood. Staffs owe it to their CGs to capture and operationalize risk management to preserve combat power and achieve the mission.

During the fifth warfighter exercise for the protection observer, coach/trainer team, Mission Command Training Program, U.S. Army Combined Arms Center, Fort Leavenworth, Kansas, it was the job of Operations Group Alpha to train the division protection staff to keep the combat power alive. However, the enemy always has a say during combat operations and the observer, coach/trainer team observed that the same combat power losses encountered in previous warfighter exercises were manifesting themselves again. The division CG directed the protection cell to update the critical asset list/defended asset list[2] and reevaluate the air defense scheme, but losses continued. The division protection chief, dutifully following the Army risk management model, identified many battlefield hazards, articulating each on his risk matrix. Enemy fixed-wing; rotary-wing; and chemical, biological, radiological, and nuclear weapons were captured, assessed, mitigated, and assigned residual risk. Yet, losses continued to occur at an unacceptable rate. The staff captured enemy threats, but friendly combat power losses continued to surprise the staff and CG. Why was the staff failing to anticipate where losses would be taken? And why was it struggling to do something to stop them? What could the staff do to better understand the risk to combat power? These questions drove the protection observer, coach/trainer team to examine the Army's risk assessment model in detail. What emerged is a method that, if employed properly, will be effective at determining risk for division and corps level operations, providing input for the CG's FFIR, and operationalizing the risk management process.

Current Army Risk Assessment Model

Before exploring new ways to visualize risk for divisions and corps, the way in which the Army currently conducts risk assessment should be examined. Army Techniques Publication (ATP) 5-19, *Risk Management*,[3] outlines risk assessment and management using the identify, assess, control, implement, and supervise methodology (Figure 1, page 24). The identification of hazards involves listing the environmental threats that can cause harm. The subsequent assessment of the hazards is described in ATP 5-19 and

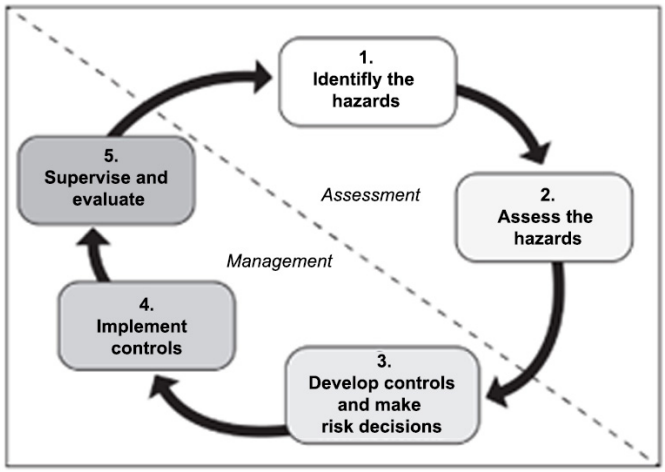


Figure 1. Current Army risk assessment and management methodology

outlined in Table 1. The Army model for risk assessment is based on two criteria: the probability and the severity of an event. Staff can use the risk assessment matrix presented in Table 1 to qualitatively evaluate the initial risk inherent to a specific hazard. Once the assessment is complete, one or more of the following types of controls are developed:

- Educational controls, which inform CGs that a hazard exists.
- Physical controls, which block access to a hazard.
- Hazard elimination controls, which make use of engineering methods and administrative and personal protective equipment to mitigate a hazard.

CGs then implement the controls and supervise/evaluate them for effectiveness. While the current Army risk assessment model has merit, it is an "accidental" risk mitigation model (as is evident in the following two examples) and its application becomes nebulous at higher echelons.

Example 1: A Soldier's Road Trip Home

In the first example, a Soldier is traveling home by vehicle for the holidays. The associated risk assessment matrix (Table 2) illustrates that the likely hazards are a vehicle accident, a vehicle breakdown, and inclement weather. Using ATP 5-19 and Table 1, it is determined that the probability of a vehicle accident is "seldom" and the severity of an accident is "critical," while the probability is "occasional" and the severity is "moderate" for both a vehicle breakdown and inclement weather—and that the initial risk for all events is "moderate." Educational, physical, and hazard elimination controls are then implemented (via the chain of command) to mitigate the risk, leaving an overall residual risk of "low." In this way, the CG is informed of events that the Soldier may encounter and a plan is developed in case a hazard is encountered. While the subjective nature of this type of assessment can be argued, the model holds up well when applied to an individual Soldier. Indeed, it holds up well even when applied at the squad to company level. However, the applicability of the model breaks down when transitioning to higher echelons.[4]

Example 2: Division Wet-Gap Crossing in LSCO

For the second example, the current Army risk management model is applied to a division conducting a wet-gap crossing in LSCO (Table 3). Vital hazards present during attack are identified; enemy rotary-wing aircraft and enemy artillery hazards are assessed as "frequent" and "catastrophic," and a chemical attack hazard is assessed as "likely." The initial risk is assessed as "extremely high." Physical and hazard response controls are implemented through the order process, leaving a residual risk of "high."

Limitations of Current Risk Model

The risk assessment model is a tool that should be used to inform the CG. But what information does it provide to the CG? In most cases, the CG has more than 25 years of military experience—yet, he is effectively told simply that "War is dangerous." The current model does not provide the CG with information about risk in time or space or about purpose—nor does it provide him with information on which to base decisions. But criticism

Risk Assessment Matrix		Probability *(expected frequency)*				
		Frequent: Continuous, regular, or inevitable occurrences	**Likely:** Several or numerous occurrences	**Occasional:** Sporadic or intermittent occurrences	**Seldom:** Infrequent occurrences	**Unlikely:** Possible occurrences but improbable
Severity *(expected consequence)*		A	B	C	D	E
Catastrophic: Mission failure, unit readiness eliminated, death, unacceptable loss or damage	I	EH	EH	H	H	M
Critical: Significantly degraded unit readiness or mission capability; minor injury, loss, or damage	II	EH	H	H	M	L
Moderate: Somewhat degraded unit readiness or mission capability; minor injury, illness, loss, or damage	III	H	M	M	L	L
Negligible: Little or no impact to unit readiness or mission capability; minimal injury, loss, or damage	IV	M	L	L	L	L
Legend: EH—extremely high risk H—high risk M—moderate risk L—low risk						

Table 1. Risk assessment matrix

Driving Home for Holidays (600 miles one way)				
Hazard	Initial Risk Level	Control	How to Implement	Residual Risk Level
Vehicle Accident	M	Rest breaks/2-day trip/ 8 hours sleep/no alcohol	Commander/NCO briefing and supervision	L
Vehicle Breakdown	M	Vehicle inspection/cell phone on-hand/hotel funds	Commander/NCO briefing and supervision	L
Inclement Weather	M	Weather assessment/ emergency hotel plans/blanket, water, food in car	Commander/NCO briefing and supervision	L

Legend:
L—low
M—moderate
NCO—noncommissioned officer

Table 2. Soldier holiday risk assessment matrix

Offensive Operations				
Hazard	Initial Risk Level	Control	How to implement	Residual Risk Level
Enemy rotary-wing aircraft	EH	Avengers task-organized to BCTs	Orders process	H
Chemical attack at the gap	EH	CBRN reconnaissance, decontamination units task-organized to BCTs; PPE utilized	Orders process	H
Enemy artillery	EH	Survivability movements conducted, survivability positions constructed, deception operations performed	Orders process	H

Legend:
BCT—brigade combat team
CBRN—chemical, biological, radiological, and nuclear
EH—extremely high
H—high
PPE—personal protective equipment

Table 3. Division wet-gap crossing risk assessment matrix

of any existing paradigm must be accompanied by suggestions for a solution or better process.

Paradigm Change—A Different Way of Looking at Risk

To preserve limited combat power, staff should think differently about how it addresses battlefield hazards. The Project Management Institute (PMI)© presents a risk mitigation paradigm that is suitable for division and corps level operations.[5] According to the PMI paradigm, risks should be avoided, eliminated, and/or mitigated (in that order) before the CG accepts residual risk (Figure 2). Too often, staffs seek to mitigate hazards before they try to avoid and/or eliminate them.

Using the PMI model, each WFF is integrated into the risk management process. The intelligence WFF helps the CG avoid risk by providing information about where the enemy is strong and where it is weak or where critical battlefield systems are arrayed. The

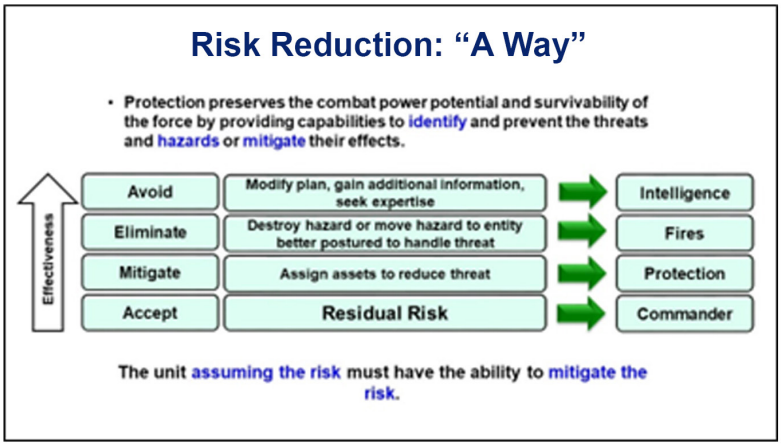


Figure 2. Risk reduction

fires WFF eliminates systems that can destroy friendly combat power, thereby reducing overall hazards to the force. The protection WFF arrays combat power to assist in survivability and mitigate the risk. Combat power is assigned as a last resort so that CGs can focus assets at the decisive point. Finally, after avoidance, elimination, and/or mitigation, the CG accepts the residual risk. The CG owns the risk for his unit; however, the staff must manage it.

According to Sun Tzu, "If you know the enemy and know yourself, you need not fear the result of a hundred battles."[6] The U.S. Army struggles with the latter of these two elements. The staff exists to inform the CG and assist him in making decisions. The information that the CG deems necessary for him to make informed decisions is codified in the CG's critical information requirements, which are broken down into two subsets—PIRs, or what we need to know about the enemy, and FFIR, or what we need to know about ourselves.

Through intelligence preparation of the battlefield, the staff determines the likely actions, locations, and strength of the enemy. It then develops a collection plan in which named areas of interest are directly linked to PIRs, which—for divisions or corps—are generally listed in great detail. The collection plans are phased, contain assigned assets for collection, and are linked to CG decision points. This is not shocking, as tactical intelligence efforts focus on PIRs. CGs and their staffs also have the doctrine to drive the CG's decision-making cycle. ATP 2-01, *Collection Management*,[7] specifically addresses how to develop plans to address PIRs.

FFIR are another matter. Staffs often need to define who is responsible for developing and tracking FFIR. Is that the role of the protection staff? Or does that responsibility reside with the operations section? Unlike PIRs, FFIR are typically not phased, do not drive decisions, and are not depicted on the decision support matrix. In short, FFIR generally do not provide the CG with effective or timely information. Take a moment to develop FFIR for a division attack in LSCO. Think about what the CG needs to know about his forces, how to maintain combat power, and how FFIR would impact the mission based on your experience. Your FFIR likely include at least two of the following effects on friendly equipment:

- Loss of an Avenger platoon.
- Loss of counter-fire radar.
- Loss of an Apache platoon or higher.
- Loss of a chemical, biological, radiological, and nuclear reconnaissance vehicle.

How can FFIR be so quickly and accurately determined? Could the same exercise be conducted with PIRs? The simple fact is that we are products of our development. We list these particular FFIR because we learned them from the executive officer (S-3) who trained us as junior officers. And he learned FFIR development in the same way. While equipment systems such as Avengers; counter-fire radar Apaches; and/or chemical, biological, radiological, and nuclear vehicles are surely important to the CG, does their loss really inform him of anything? Again, the CG likely has more than 25 years of service. He understands that the loss of an Avenger platoon is bad. Does this information contribute to his decision making? The answer is no. So, how can we develop effective FFIR?

Risk Management During the Decision-Making Process—The Key to Informed FFIR

Effective risk management is key to developing updated, phased, and living FFIR. Risk management must begin during mission analysis; it cannot be an afterthought. The step-by-step process of one effective technique can be used to assess risk for division offensive operations in LSCO and turn risk modeling into actionable FFIR that can contribute to decision making.

Step 1 of the risk assessment/FFIR development process, which takes place during mission analysis, is to assign the responsibility of managing the risk matrix to a WFF. By doctrine, this role is filled by the protection WFF; however, as long as a single party is deemed responsible, the process will be successful. For the purpose of this article, the protection WFF will serve as the responsible party for the risk matrix.

Risk to mission and force statements should be included on all WFF running estimates. During mission analysis, the protection cell captures any risk that the WFFs identify (Table 4). At this point, there is no risk assessment; there is simply an identification of hazards in the operational environment. Their impact on the force is noted; but at this phase of planning, the impacts are broad. The WFF that identified the risk is also captured. That WFF will own the risk for the duration of the operation. The purpose of risk management during the mission analysis portion of the decision-making process is for the staff to brainstorm where it envisions threats. The staff does not assign assets to "mitigate" the threat.

Step 2, which takes place during course of action (COA) development, builds on mission analysis activities. During COA development, the staff develops broad, phased concepts from initiation of movement to achievement of the final objective. Expansion of the risk model begins, and the number of columns in the COA matrix (Table 5, page 28) increases over that of the mission analysis matrix. A column for the operational phase is now included. Also included is a column for probability, which contains a subjective assessment of the likelihood of event occurrence. By this phase of planning, the staff should have a fair idea of when the division or corps will encounter a certain hazard. The staff can now begin to formulate how to reduce the hazard. Will it be avoided, eliminated, and/or mitigated? As planning progresses, additional hazards will likely become evident. These hazards—along with the dates the hazards are identified—should be noted on the risk matrix. For example, the first row of Table 5 (page 28) indicates that on 3 June 2019, it was determined that the main effort brigade combat team (BCT) would be reduced to 65 percent combat power before crossing

Mission Analysis—Division Offensive Operations				
WFF Risk Target	Hazard	Impact	Risk to Mission	Risk to Force
Protection/M2	Rotary-wing attack	Tempo		
Fires	Enemy indirect fires	Tempo/OPREACH		
Protection	Chemical attack	Tempo/OPREACH/ basing—all reduced		
MC/protection	Cyber attack	OPREACH		
M2	Enemy unconventional attacks in support areas	Tempo/OPREACH/ basing		

Legend:
M2—movement and maneuver
MC—mission command
OPREACH—operational reach
WFF—warfighting function

Table 4. Example of a mission analysis risk matrix

the gap. Quantitative data, which is often derived from operations research/systems analysis, is extremely useful during COA analysis. WFF chiefs should examine the risk assessment matrix and determine how risks incurred from one function may impact another. Using the example of the main effort BCT at 65 percent combat power, leaders of the sustainment WFF can infer that there is a significant risk for a mass casualty event and task-organize to mitigate this hazard.

By the time the staff reaches Step 3 of the process, the risk matrix should be specific to the situation. At this stage, during COA analysis (wargaming), the WFF has determined second-order effects and is now prepared to plan in detail. The COA analysis risk matrix delineates phases. Some hazards are present throughout the operation; however, it is important to note how they will affect the mission during critical events. Also included in the COA risk matrix are risk-to-mission and risk-to-force columns; the intent is to show how the controls affect risk and where significant risk will still be incurred by the division. In the case of the 65 percent combat power loss of the main effort BCT, the Phase III wet-gap crossing is a key event for the division. During wargaming, branch plans are identified and, in some cases, developed in order to execute when FFIR are triggered. The focus is now on the actual units to which the staff assigned missions.

In Step 3, risk management focuses on avoiding, eliminating, and/or mitigating risk. For example, if division artillery is unable to provide effective fires to the support coordination line, risk can be avoided by positioning fires assets farther ahead in the order of march. The hazard could concurrently be eliminated by coordinating with the joint force CG to shift the fire support coordination line for this phase of the battle, if permissible—which could impact targeting.

Some hazards cannot be avoided or eliminated. For example, the division does not have the ability to prevent a chemical, biological, radiological, and nuclear attack. However, through task organization and the orders process, it can mitigate the corresponding reduction in tempo and casualty threat. By this point in the process, the protection chief should have a good product for facilitating action/reaction planning during key events. The protection chief provides the risk matrix to the chief of staff as input for adjudication. This can drive additional decisions. For example, if the reduction of the main effort BCT to 65 percent combat power is deemed too low for adequate correlation of forces, this may drive changes to targeting or support from higher headquarters and provide input for the development of branch plans. In this example, a branch plan may address the shifting of the main effort during Phase III of the operation.

This risk management process provides the science needed to drive the chief of staff's adjudication during wargaming. Through the adjudication process, the staff may determine that, due to the friendly combat power situation, the plan cannot continue unaltered. For example, if friendly combat power losses result in unfavorable correlation-of-forces ratios, targeting may need to focus on a given enemy asset or formation to allow the operation to continue. As always, we hope for the best but plan for the worst. If the staff determines that a friendly combat power

WFF Risk Target	Operation Phase	Date/Time Risk Identified	Hazard	Impact	Probability	Avoid	Eliminate	Mitigate	Risk to Mission			Risk to Force		
C2	IIIb–Gap Crossing	3 Jun 19	ME BCT reduced to 65 percent combat power before crossing	Tempo/ Casualties	High—Enemy COF not favorable		X	X						
Fires	IIIb–Gap Crossing	3 Jun 19	CL V exceeds CSR to shape follow-on objective	Tempo/ OPREACH	Medium	X		X						
Prot/M2	IIIb–Gap Crossing	1 May 19	Rotary-wing attack along northern flank	Flank attack pot. Fix in north	High—RW assets at 85 percent		X	X						
Fires	IIIa–IIIc	1 May 19	Enemy indirect fires	Tempo/ OPREACH	Medium—enemy has overmatch in range	X	X	X						
Prot	IIIb–Gap Crossing	1 May 19	Chemical attack	Tempo/ OPREACH/ basing—all reduced	Likely—already used 90 percent			X						
C2/Prot	IIIa–IIIc	1 May 19	Cyber attack	OPREACH	Medium—40 percent			X						
C2	IIIc	1 May 19	Enemy unconventional attacks in support areas	Tempo/ OPREACH/ basing	Likely—already used 90 percent		X	X						

Legend:
BCT—brigade combat team
C2—command and control
CL—class
COF—correlation of forces
CSR—controlled supply rate
M2—movement and maneuver
ME—mechanized
OPREACH—operational reach
pot—potential
Prot—protection
RW—rotary-wing
WFF—warfighting function

Table 5. Example of a COA development risk matrix

loss presents significant risk to the mission or force, a decision point is reached and a branch plan is developed to meet the CG's intent. These FFIR-driven decision points are captured on the decision support matrix. The risk management process does not end here; it continues to develop, with staff sections maintaining risk as part of their running estimate. The protection working group serves as an excellent venue for consolidating staff risk assessments, briefly focusing the staff on the question of "What is killing us?" The tools are now in place to inform the CG of the risk and the actions that he may need to take.

The "Field Grade Product" Versus the "CG's Product"—FFIR Input to the CG's Decisions

At this point, hazards starting at the receipt of the mission have been identified and cross-functionally screened and second- and third-order effects have been developed. Indeed, many of the second- and third-order effects have themselves become hazards added to the risk matrix. The best, most efficient way to control a risk through avoidance, elimination, and/or mitigation has been determined. Finally, an updated risk matrix has been presented to the chief of staff as input for his adjudication. Decision points have been developed, and they are now included in the decision support matrix.

Now, risk must be presented to the CG in a usable format. The detailed risk matrix that has been developed is the "field grade" product. It undergoes constant refinement. However, staff members who hand this product off to the CGs do not generally remain on the staff very long. In spite of this, CG briefings contain the field grade risk matrix time and time again. No wonder risk is glanced over! The field grade risk matrix does not help the CG visualize, describe, or direct the battle. Risk must be presented to the CG in a way that helps him see it in time, space, and purpose.

At this point, the risk matrix is likely relatively large. Now is the time to focus on key risks and reduce the size of the matrix over the course of the next few days. Key risks, which should be presented at the daily battle update briefing, include—

- Risk with a linked decision point.
- Risk that cannot be directly influenced by the division or corps.
- Risk that can cause culmination.
- Risk with political consequences.

These key risks should be listed on a reduced form of the risk matrix. All extraneous information should be removed, and the risk should be expressed in terms of risk to mission and risk to force. Since this is primarily a qualitative assessment, the expert judgement of the staff should be used

to refine the product. Staff recommendations for controlling the risk through avoidance, elimination, and/or mitigation should be expressed. In cases for which the division cannot directly influence the risk, the term "transfer" should be used to indicate that coordination with a higher echelon is necessary. Coordination with the corps would be required in order to transfer the risk. The corps is postured to control the hazard; such control is critical for the operation.

An updated common operating picture should be included on a presentation slide, and a symbol should be placed where the staff believes the division will encounter the risk. This will help the CG visualize where mission hazards are expected to be encountered. This is not a decision support product, so care must be taken to avoid confusing the CG. Many—but not all—risks have a decision point associated with them.

To complete the CG's product, an example from the risk model should be used to show when the division will encounter the risk. The risk example should be laid out in terms of risk to mission, risk to force, and political risk. Some risk elements will be classified as all three. The assessment should be used to determine the best fit spatially. Links among hazards should also be made. The hazards are now presented to the CG in time, space, and purpose. He can now see how his force may be impacted. He can now "know himself."

Step 4, the final step in the process, is to inform the CG of the FFIR and associated decision points. FFIR are expressed as refined, detailed statements that link risk to combat power losses, which in turn requires decisions. The risk that requires decisions is presented in a concise statement. We have now provided the "then" statement to the division or corps decision support matrix with the homework to back up our assessment, and the CG now knows what friendly combat power decisions will need to be made to meet his intent. This method in which risk management drives FFIR and associated decision points can be used to better inform the CG, enhance mission accomplishment, and preserve the valuable lives of our Soldiers.

Conclusion

Risk management must move beyond identifying hazards, applying mitigation, and accepting residual risk. An integrated, whole-of-staff risk management approach to identifying, avoiding, eliminating, and/or mitigating hazards is crucial to correctly defining the operational environment as it changes during LSCO. Capturing risk and managing it for the entire staff should start with mission analysis, undergo testing through harsh adjudication during wargaming, and be maintained as part of the staff running estimate. The staff estimates should be consolidated and discussed during protection working group meetings to further refine upcoming hazards. Risk should be presented to the CG in time, space, and purpose to assist him in visualizing battlefield hazards and making decisions. Division and corps staffs must improve upon current risk management models/methods in order to reduce the risk to mission and force to the minimum residual level that allows the CG to preserve and maximize the effects of his combat power.

Endnotes:

[1]ADP 6-0, *Mission Command: Command and Control of Army Forces*, 31 July 2019.

[2]Current doctrine uses the overarching term of Protection Prioritized List (PPL). (ADP 3-37, *Protection*, 31 July 2019.)

[3]ATP 5-19, *Risk Management*, 9 November 2021.

[4]Ibid, p. 1-7

[5]David Hillson, "Managing Overall Project Risk," paper presented at PMI Global Congress 2014—European Middle East and Africa, Dubai, United Arab Emirates. Newtown Square, Pennsylvania, Project Management Institute, 2014, <https://www.pmi.org/learning/library/overall-project-risk-assessment-models-1386>, accessed on 10 October 2023.

[6]Sun Tzu, *The Art of War*, 5th Century B.C., with translation and commentary by Lionel Giles, Capstone Publishing, 2022.

[7]ATP 2-01, *Collection Management*, 17 August 2021.

Lieutenant Colonel Gervais (Retired) is the former protection chief of Operations Group Alpha, Mission Command Training Program, U.S. Army Combined Arms Center, Fort Leavenworth, Kansas. He holds a bachelor's degree in biology from Purdue University and a master's degree in environmental management from Webster University. He is also a graduate of the U.S. Army School of Advanced Military Studies, Fort Leavenworth.

Lieutenant Colonel Brookshire is the protection chief and provost marshal for the 1st Infantry Division, Mission Command Training Program. He is the former executive officer of the Mission Command Training Program. He holds a bachelor's degree in psychology from the University of Maryland; a master's degree in business and organizational security management from Webster University; and a graduate certificate in administration from Central Michigan University, Mount Pleasant.

Taming the Hydra:

Working Toward an Integrated Protection Construct

By Mr. Stephen D. Carey, Ms. Melissa E. Chadbourne, and Colonel Barrett K. Parker (Retired)

Land power ends wars. The breakneck pace with which disruptive technology is changing the operating environment—breaking down the distinctions between competition and conflict—does not change the fundamental truth that no matter how the next large-scale war among great powers starts and is fought, it will end with a decisive land campaign. When the U.S. Army can project force in time and at scale, the joint force commander is overwhelmingly capable of finishing the fight. Our adversaries know this, and they are taking measures intended to prevent the Army from globally projecting massed ground forces. If the Army can successfully defend against aggressive behaviors that threaten its programs, facilities, and personnel here at home, then we can ensure that the Army is ready and able to deploy and project force at a place and time of our choosing—not that of our adversaries. To ensure decisive force projection, the Army must reframe and reform its dis-integrated protection functions into an integrated protection construct.

In the time that it takes to read this article, advanced U.S. capabilities will confront and counter a multitude of threats such as artificial intelligence, machine learning, advanced cyber operations, or adversarial social media mis/disinformation campaigns, only to see additional threats emerge and multiply. As with the hydra of antiquity, attempts to defeat the technological drivers of today's military modernization often expose friendly advanced capabilities and sources, increasing the opportunity for further technology-driven disruption.[1] Our adversaries deliberately employ these disruptive technologies in support of hybrid warfare strategies that avoid direct conflict with U.S. military power,[2] intentionally blurring the distinction between competition and conflict.[3] This ambiguous environment enables foreign security and intelligence organizations to actively collect information about our installations, networks, systems, and critical infrastructure and to test them to prevent us from projecting forces forward in a future armed conflict. By targeting our efforts in our homeland, our adversaries have brought the fight to us and are setting conditions in their favor to interrupt our ability to mobilize, deploy, and win a large-scale war.

China and Russia are currently collecting information about U.S. Army modernization by using advanced and emerging technologies, cyberspace operations, and information capabilities.[4] Their actions have recently been demonstrated within the United States and around the world, and they continue to evolve. Although unmanned aerial vehicles or drones have been used since the Vietnam War,[5] unmanned, commercially produced drones are now being used to deliver lethal strikes in armed conflicts. In 2017, Russian forces used a drone to target an ammunition dump in Ukraine, resulting in approximately $1 billion worth of damage,[6] while Ukrainian forces have "used 3D printers to add tail fins to Soviet-era antitank grenades that were then dropped from an overhead commercial drone to target Russian tanks and vehicles."[7] New technologies continue to help advance the applications of unmanned systems that use artificial intelligence for command and control. In 2020, China tested a "swarm of loitering munitions, also often referred to as suicide drones . . . [which] underscores how the drone swarm threat, broadly, is becoming ever-more real and will present increasingly serious challenges for military forces around the world in future conflicts."[8]

Cyberspace operations further enable a multitude of attack vectors that may be capable of targeting communications systems or exfiltrating information. In 2019, a "denial-of-service attack on [an] encrypted messaging-service telegram disrupted communications among Hong Kong protestors."[9] And at the start of the Russian invasion of Ukraine in 2022, an attack on a satellite broadband service disrupted Internet services across Europe and affected Ukrainian military communications.[10] Our adversaries exploit the global nature of Internet communications and social media by using networks of state media, proxy shells, and social-media influence actors who disseminate false content or amplify information that is beneficial to their efforts to influence.[11] For example, Russian propaganda portrays Russian attacks against Ukraine as being more powerful than they actually were, thereby creating the false illusion that Ukraine is not fighting back.[12] And Chinese influence operations have highlighted the 2023 Ohio train derailment that resulted in the release of toxic chemicals and alleged that the United States was involved in the 2022 sabotage of pipelines used to transport Russian gas.[13] These challenges in the operating environment—both in the homeland and abroad—are only expected to intensify as we look toward 2040 and beyond.

According to General James E. Rainey, commanding general of the U.S. Army Futures Command, in future conflicts, "We are going to be fighting under constant observation and in some form of contact at all times. The enemy is going to be able to see us somewhere—electromagnetic spectrum, digitally, from space."[14] This new transparent battlefield will be a further challenge to Army protection efforts, requiring additional countermeasures and incorporating more data and advanced analytics to support informed decision making. Addressing these changes to the operational environment, General Rainey stated, "[This] needs to translate into every modernization effort, but more importantly into our tactics and doctrine."[15]

For those operating in Army protection programs, activities and operations have historically been divided between warfighting and nonwarfighting functions. These divides are causing inefficiencies in how the Army conducts protection. The truth is that there are no "nonwarfighting" functions. Everything the Army does directly contributes to supporting the fight and the warfighter. We need to stop thinking about the homeland as a place where we are at rest and in relatively safety. If we truly subscribe to the concept that our installations and garrisons in the United States are under daily threat by our adversaries, then we must treat the mislabeled "nonwarfighting" protection functions as a critical part of our warfighting efforts. We must bring the warfighting and nonwarfighting protection programs together in a way that seamlessly integrates the actions across the conflict continuum. Only by harnessing the multitude of protection functions and programs under an overarching structure can we ensure that the Army can adapt to the evolving threat landscape and rise to meet future challenges. Therefore, we propose that the Army dramatically rethink protection across the entire range of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy solutions, beginning with synchronized strategies and implementation plans that support the Army of 2030 and are aligned with the requirements for the Army of 2040.

The warfighting protection functions are currently synchronized by the U.S. Army Maneuver Support Center of Excellence (MSCoE), Fort Leonard Wood, Missouri, through Army Doctrine Publication (ADP) 3-37, *Protection*,[16] while the nonwarfighting protection functions are coordinated through the Army Protection Program, which is managed by the Directorate of Operations, Plans, and Training (G-3/5/7), Headquarters, Department of the Army, Washington, D.C., and described in Army Regulation (AR) 525-2, *The Army Protection Program*.[17] As indicated in Figures 1 and 2 (page 32), there is a high degree of similarity between the protection function tasks (ADP 3-37) and the primary and enabling protection functions (AR 525-2), although they each contain unique requirements and activities. Indeed, ADP 3-37 references the Army Protection Program to ensure doctrinal consistency between the two guiding documents. While these two aspects of protection are actively undergoing adaptations and adjustments to meet the range of current threats, more work must be done to bring them closer together to prepare the Army for the threats and challenges that it will inevitably face in the future.

One challenging aspect of Army regulations and doctrine (including AR 525-2 and ADP 3-37) is the need for frequent updates. Discussions about whether the next iteration should add, subtract, modify, or rename protection functions (or tasks) in keeping with emerging threats and

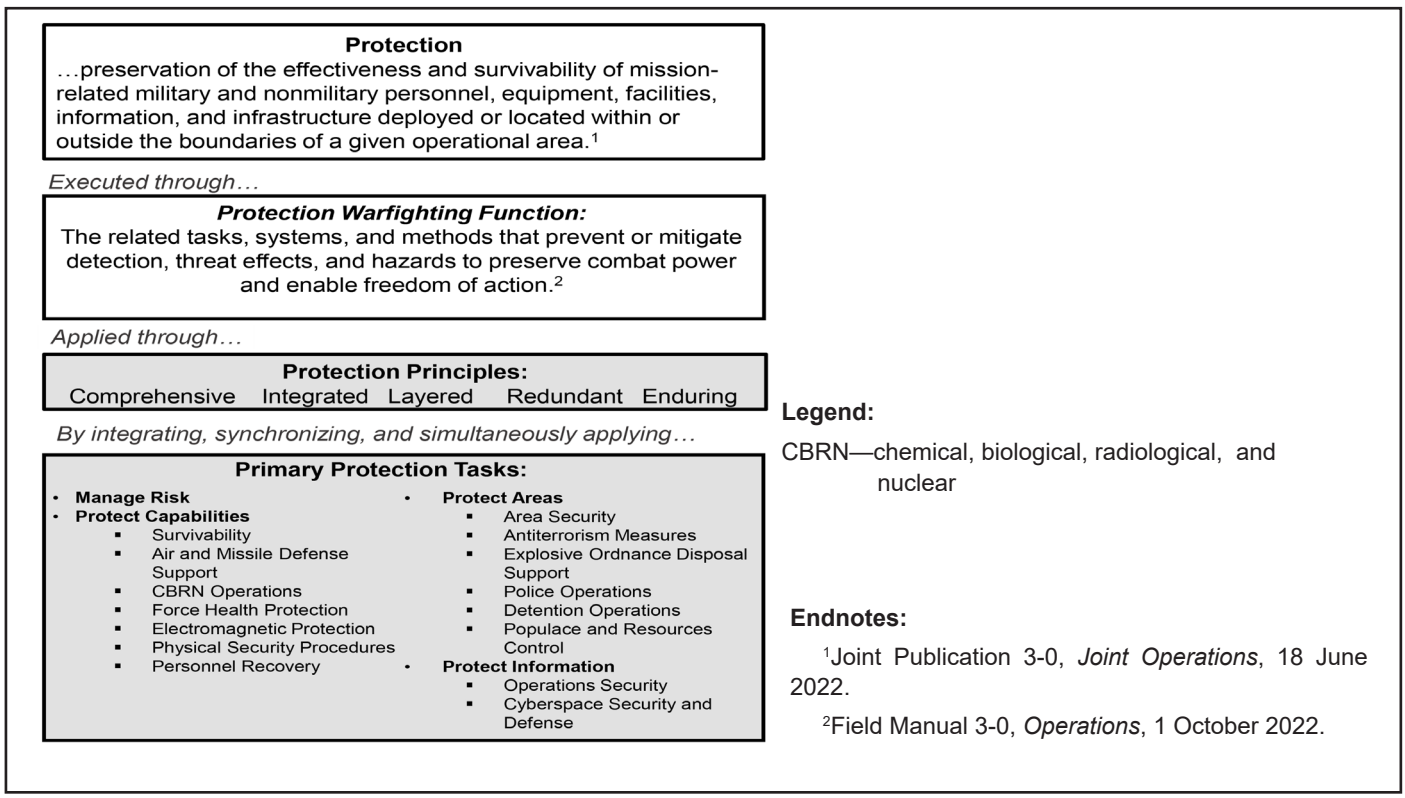


Figure 1: Protection logic map

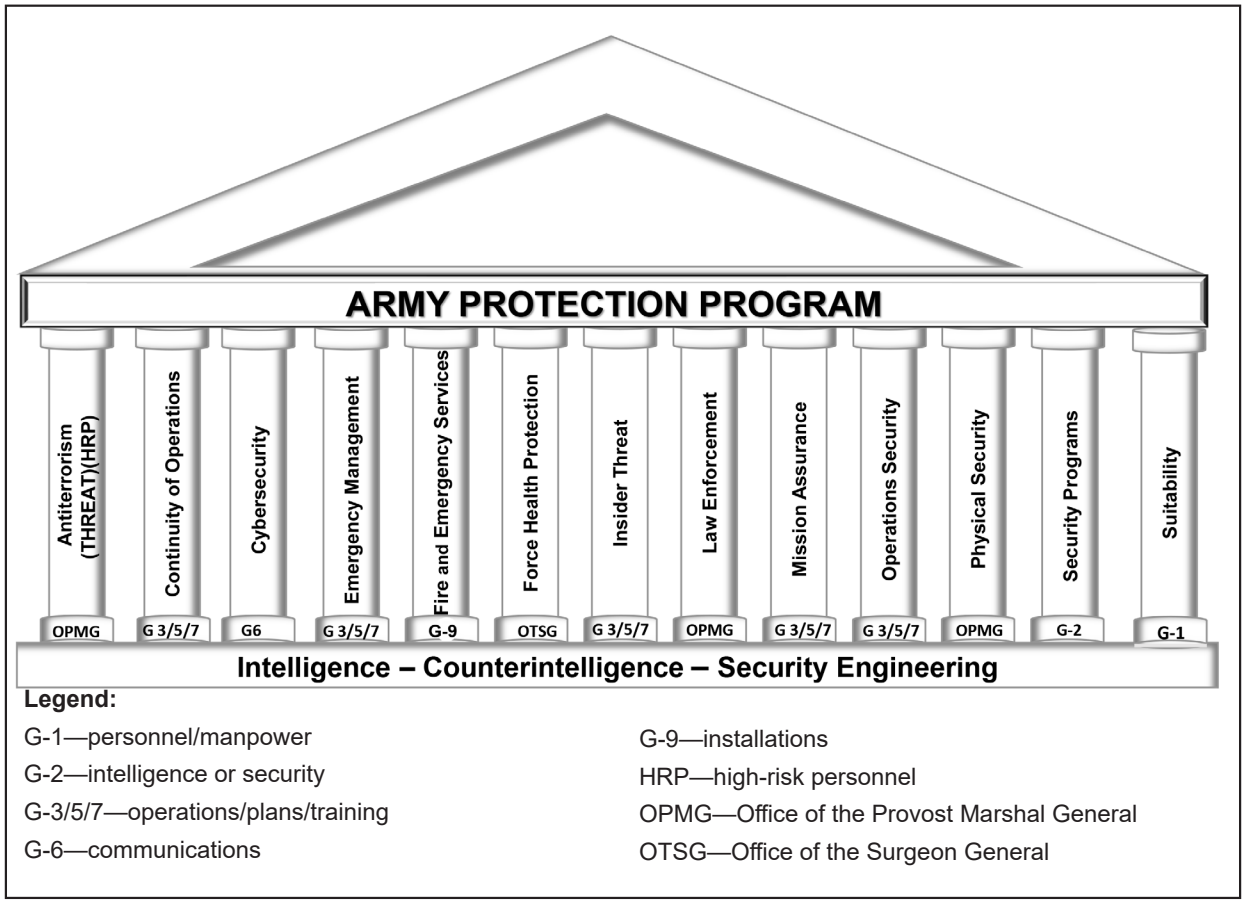


Figure 2: The Army Protection Program[18]

the goals of Army future concepts are never-ending. While the exact tasks to be listed are valid considerations, a bigger concern than what constitutes Army protection efforts is how the Army approaches protection. As previously mentioned, there are many similarities between warfighting and nonwarfighting protection functions and ADP 3-37 guidance references the Army Protection Program, but there is no clearly defined point at which an activity transitions from "nonwarfighting" to "warfighting." Army protection currently operates in two friendly siloes—each operation is aware of the other, but they are not fully integrated. We instead propose a new integrated protection strategic construct—something along the lines of what is shown in Figure 3, in which the transitions between "nonwarfighting" and "warfighting" are blurred along the competition continuum. An integrated construct would align protection activities with the Army 2040 requirements to fight in a transparent and contested environment.

The challenges of current and future operating environments will disrupt the Army across all domains and through all stages of force generation, modernization, readiness building, and force projection. As our adversaries exploit the competition phase with relative freedom of maneuver in the homeland, they could potentially create conditions that impede the Army from modernizing and projecting forces. We seek to prevent these activities and ensure the effective and seamless operation of Army protection functions across the blurry lines between competition and conflict.[19] To provide ground forces that can sustain the fight across contested terrain and over time, Army protection efforts must ensure that Army forces progress from generating capability to delivering battlefield effects, unimpeded by adversary efforts that span the competition-conflict continuum.[20] Achieving that goal requires a deliberate and concerted effort in terms not only of directing resources toward modernization and readiness activities but also of considering how we protect the personnel, programs, systems, and information that enable Army forces to prepare for deployment. Integrating the dis-integrated functions of Army protection will enable the Army to meet and overcome the challenges intended to impede Army forces from getting to the fight.

We are undertaking this challenge with deliberation and a willingness to rethink our past approaches in order to be positioned for the future. The Army Protection Division, Headquarters, Department of the Army, has begun reforming the Army Protection Program to address problems arising from current threats, vulnerabilities, and hazards. Looking to the near future, Headquarters, Department of the Army, and MSCoE must unite protection activities under an integrated protection construct that supports the full range of protection activities across the full spectrum of conflict, from fort to port to theater. This construct will drive doctrine and policy revisions that have a coordinated approach to the way forward and are linked to the future concepts being developed by the Army Futures Command. This also means that the new strategy will be

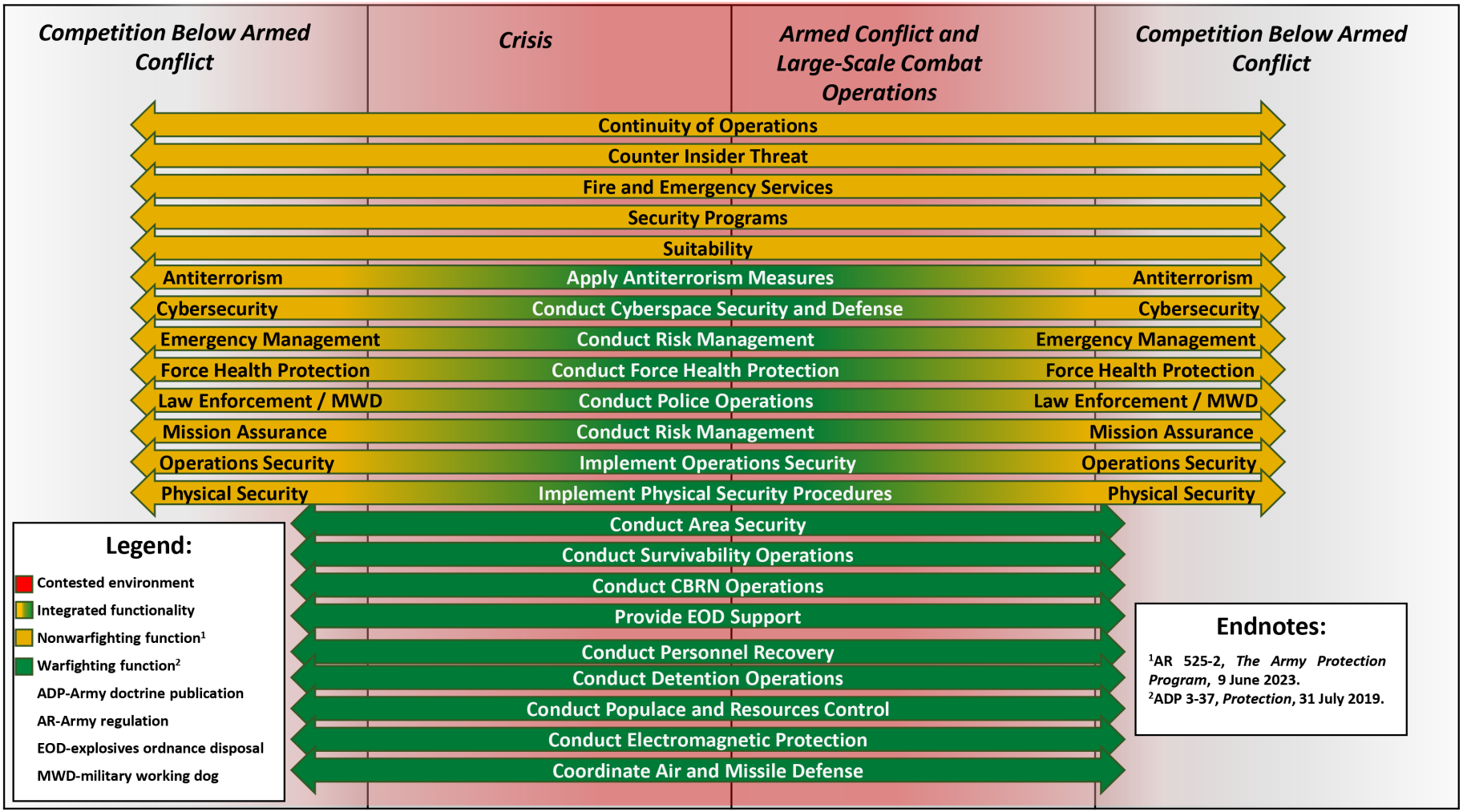


Figure 3. Protection Support Throughout the Army's Strategic Context

implemented using the full range of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy concepts to further influence the Army enterprise. By adapting programs, policies, training, and exercises to address current threats, we can better adapt for emerging threats and better position the Army to project force to fight in a contested and transparent environment. If the Army fails at protection, we fail at projection. Only by designing a new integrated protection construct that effectively links the full range of protection activities will we fully support the Army of 2040 and beyond.

Endnotes:

[1]David Petraeus, "CyCon 2019 Twilight Talk," <https://www.youtube.com/watch?v=KyCDvEzq25s>, accessed on 16 August 2023.

[2]Clementine Starling et al., "Today's Wars Are Fought in the 'Gray Zone.' Here's Everything You Need to Know About It," Atlantic Council Hybrid Conflict Project, 23 February 2022, <https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/>, accessed on 16 August 2023.

[3]Nathan P. Frier et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone*, Strategic Studies Institute and the U.S. Army War College Press, Carlisle, Pennsylvania, June 2016, p. 3.

[4]Field Manual (FM) 3-12, *Cyberspace Operations and Electromagnetic Warfare*, 24 August 2021.

[5]"A Brief History of Drones," Imperial War Museum, <https://www.iwm.org.uk/history/a-brief-history-of-drones>, accessed on 16 August 2023.

[6]Kyle Mizokami, "Kaboom! Russian Drone With Thermite Grenade Blows Up a Billion Dollars of Ukrainian Ammo," *Popular Mechanics*, 17 July 2017, <https://www.popularmechanics.com/military/weapons/news/a27511/russia-drone-thermite-grenade-ukraine-ammo/>, accessed on 16 August 2023.

[7]Gregory C. Allen, "Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine," Center for Strategic and International Studies (CSIS), 13 May 2022, <https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine>, accessed on 16 August 2023.

[8]Joseph Trevithick, "China Conducts Test of Massive Suicide Drone Swarm Launched From a Box on a Truck," *The Drive*, 14 October 2020, <https://www.thedrive.com/the-war-zone/37062/china-conducts-test-of-massive-suicide-drone-swarm-launched-from-a-box-on-a-truck>, accessed on 16 August 2023.

[9]"Significant Cyber Incidents Since 2006," CSIS, <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>, accessed on 16 August 2023.

[10]Ibid.

[11]"Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, 6 February 2023, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>, accessed on 16 August 2023.

[12]Jason Abbruzzese, "Russian Disinformation, Propaganda Ramp Up as Conflict in Ukraine Grows," *NBC News,* 24 February 2022, <https://www.nbcnews.com/author/jason-abbruzzese-ncpn843466>, accessed on 17 August 2023.

[13]Nomaan Merchant and Matthew Lee, "U.S. Sees China Propaganda Efforts Becoming More Like Russia's," Associated Press, 7 March 2023, <https://apnews.com/article/china-russia-intelligence-foreign-influence-propaganda-0476f41aa932cd4850627a7b8984baa2>, accessed on 17 August 2023.

[14]Dan Barkin, "Four-Star Army General Says Technology Changing War Strategies," *Business North Carolina*, 31 July 2023, <https://businessnc.com/four-star-army-general-says-technology-changing-war-strategies/>, accessed on 17 August 2023.

[15]Laura Heckman, "Just In: Army Futures Command Shifts Focus to 2020," *National Defense*, 8 February 2023, <https://www.nationaldefensemagazine.org/articles/2023/2/8/army-futures-command-shifts-focus-to-2040>, accessed on 17 August 2023.

[16]ADP 3-37, *Protection*, 31 July 2019.

[17]AR 525-2, *The Army Protection Program*, 9 June 2023.

[18]Ibid.

[19]FM 3-12, *Cyberspace Operations and Electromagnetic Warfare*, 24 August 2021.

[20]The Army of 2030," U.S. Army, 5 October 2022, <https://api.army.mil/e2/c/downloads/2022/10/06/4632c205/army-2030-information-paper.pdf>, accessed on 16 August 2023.

Mr. Carey is the deputy division chief of the Army Protection Division, G-3/5/7, Headquarters, Department of the Army. He holds a master's degree in history from the University of Montana, Missoula, and a graduate certificate in world religions and diplomacy from George Mason University, Fairfax, Virginia. He plans to complete a master's degree in strategic studies at the U.S. Army War College, Carlisle, Pennsylvania, in 2024.

Ms. Chadbourne is a policy analyst supporting the Army Protection Division, G-3/5/7, Headquarters, Department of the Army. She holds a bachelor's degree in history from Smith College, Northampton, Massachusetts, and a master's degree in international relations from the Johns Hopkins School of Advanced International Studies, Washington, D.C.

Colonel Parker (Retired) is the deputy of the TRADOC Proponent Office–Protection, Fielded Force Integration Directorate, MSCoE. He holds a bachelor's degree in earth science from Pennsylvania State University, University Park; a master's degree in environmental management from Samford University, Homewood, Alabama; a master's degree in engineering management from Missouri University of Science and Technology at Rolla; and a master's degree in strategic studies from the U.S. Army War College, Carlisle, Pennsylvania. He retired as a colonel from the U.S. Army Reserve.

Protection Doctrine Update

"Doctrine is indispensable to an army. Doctrine provides a military organization with a common philosophy, a common language, a common purpose, and a unity of effort."

—General George H. Decker
U.S. Army Chief of Staff, 1960–1962

Number	Title	Proponent	Publication Date
ADP 3-37	*Protection*	MSCoE/USAMPS	31 July 2019
ATP 3-07.6	*Protection of Civilians*	Peacekeeping and Stability Operations Institute	29 October 2015
ATP 3-11.32	*Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Passive Defense*	MSCoE/USACBRNS	13 May 2016
ATP 3-11.36	*Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Planning*	MSCoE/USACBRNS	24 September 2018
ATP 3-13.3	*Operations Security for Division and Below*	CAC/CADD	16 July 2019
ATP 3-34.20	*Countering Explosive Hazards*	MSCoE/USAES	21 January 2016
ATP 3-37.2	*Antiterrorism*	MSCoE/USAMPS	19 July 2021
ATP 3-39.10	*Police Operations*	MSCoE/USAMPS	24 August 2021
ATP 3-39.30	*Security and Mobility Support*	MSCoE/USAMPS	21 May 2020
ATP 3-39.32	*Physical Security*	MSCoE/USAMPS	8 March 2022
ATP 3-50.3	*Multi-Service Tactics, Techniques, and Procedures for Survival, Evasion, and Recovery*	U.S. Army Personnel Recovery Proponent	5 July 2023
ATP 3-50.20	*Survival, Evasion, Resistance, and Escape (SERE) Planning and Preparation*	U.S. Army Personnel Recovery Proponent	29 November 2017
ATP 3-50.21	*Survival*	U.S. Army Personnel Recovery Proponent	18 September 2018
ATP 3-50.22	*Evasion*	U.S. Army Personnel Recovery Proponent	28 November 2017

Number	Title	Proponent	Publication Date
ATP 3-57.10	*Civil Affairs Support to Populace and Resources Control*	USAJFKSWCS	6 August 2013
ATP 3-90.4	*Combined Arms Mobility*	MSCoE/USAES	22 June 2022
ATP 4-02.8	*Force Health Protection*	MEDCoE	9 March 2016
ATP 4-32.1	*Explosive Ordnance Disposal (EOD) Group and Battalion Headquarters Operations*	CASCOM	24 January 2017
ATP 4-32.2	*Multi-Service Tactics, Techniques, and Procedures for Explosive Ordnance*	ALSSA/CADD	12 March 2020
ATP 4-32.3	*Explosive Ordnance Disposal (EOD) Company, Platoon, and Team Operations*	U.S. Army Ordnance School	1 February 2017
ATP 5-19	*Risk Management*	TRADOC Safety Office	9 November 2021
ATP 6-02.70	*Techniques for Spectrum Management*	CCoE	16 October 2019
FM 3-01	*Air Missile Defense Operations*	FCoE	22 December 2020
FM 3-11	*Chemical, Biological, Radiological, and Nuclear Operations*	MSCoE/USACBRNS	23 May 2019
FM 3-12	*Cyberspace and Electronic Warfare Operations*	CCoE	24 August 2021
FM 3-50	*Army Personnel Recovery*	U.S. Army Personnel Recovery Proponent	2 September 2014
FM 3-63	*Detainee Operations*	MSCoE	2 January 2020
FM 4-02	*Army Health System*	MEDCoE	17 November 2020
FM 6-02	*Signal Support to Operations*	CCoE	13 September 2019

All doctrine publications can be accessed at <https://armypubs.army.mil>.

The Protection Doctrine Update can also be accessed online at <https://home.army.mil/wood/index.php/contact/publications/ppb>.

Note: Users must adhere to any limited dissemination control markings that appear on publications and follow the authorized-dissemination requirements to authorized recipients only. Comments or questions about Protection doctrine can be e-mailed to <https://home.army.mil/wood/index.php/contact/publications/ppb>.

Legend:

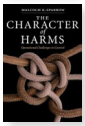
ADP—Army doctrine publication
ALSSA—Air, Land, Sea, Space Application
ATP—Army techniques publication
CAC—U.S. Army Combined Arms Center
CADD—Combined Arms Doctrine Directorate
CASCOM—U.S. Army Combined Arms Support Command
CCoE—U.S. Army Cyber Center of Excellence
EOD—explosive ordnance disposal
FM—field manual
MEDCoE—U.S. Army Medical Command Center of Excellence
MSCoE—U.S. Army Maneuver Support Center of Excellence
SERE—survival, evasion, resistance, and escape
TRADOC—U.S. Army Training and Doctrine Command
USACBRNS—U.S. Army Chemical, Biological, Radiological, and Nuclear School
USAES—U.S. Army Engineer School
USAJFKSWCS—U.S. Army John F. Kennedy Special Warfare Center and School
USAMPS—U.S. Army Military Police School

Protection Warfighting Function Professional Media List

This list is an important reference for the professional development of all protection leaders in the Army. Continuous self-development is one of the ways that we can maintain and improve our skills, challenge and refine our beliefs, and reach our full potential in an ever-changing world. These resources will improve our understanding of the protection warfighting function and its role in the diverse myriad of Army missions. These resources are intended to complement our professional military education and serve as a means of continuing education between professional military education courses. This list is a living document that is under continuous revision. Suggestions and recommendations are welcome and can be sent to <usarmy.leonardwood.mscoe.mbx.protection-fmp@army.mil>.

Protection

7 Seconds to Die, A Military Analysis of the Second Nagorno-Karabakh War, John F. Antal, Casemate, 2022, ISBN 978-1-63624-123-4. The Nagorno-Karabakh War was the first war in history to be won primarily by robotic systems, and its impact on the protection warfighting function cannot be overstated.



The Character of Harms: Operational Challenges in Control, Malcolm K. Sparrow, Cambridge University Press, 2008, ISBN 978-0521872102. This book is dedicated to the science and art of creating coherent, overarching protection programs for federal, state, and local governments and organizations faced with dozens of unrelated and sometimes highly technical protection, risk reduction, response, and safety responsibilities and efforts.

Extreme Ownership: How U.S. Navy SEALs Lead and Win, Jocko Willink and Leif Babin, St. Martin's Press, 20 October 2015, ISBN 978-1-25006-705-0. Detailing the mindset and principles that enable sea, air, and land (SEAL) units to accomplish the most difficult missions in combat, this book explains how to apply them to any team, family, or organization. Each chapter focuses on a specific topic, such as cover and movement, decentralized command, and leading up the chain, explaining what they are, why they are important, and how to implement them in any leadership environment.

Breaking Doctrine Podcast, Episode 7: "Protection," Major Chris Parker, Combined Arms Doctrine Directorate, Fort Leavenworth, Kansas, 2021, available on various podcast applications. This podcast, featuring Major General James E. Bonner (Commanding General, Maneuver Support Center of Excellence, Fort Leonard Wood, Missouri) and Brigadier General Naïve F. Knell (former Commandant, U.S. Army Military Police School, Fort Leonard Wood), discusses the protection warfighting function, one of the largest and most diverse of the warfighting functions.

AUSA 2023: Homeland Defense Seminar: The Future of Homeland Defense—Setting the Theater for Multi-Domain Operations, Army Multimedia and Visual Information Division, 10 October 2023, <https://www.dvidshub.net/video/899919/ausa-2023-homeland-defense-seminar-future-homeland-defense-setting-theater-multi-domain-operations>. Major General James E. Bonner chairs a high-level panel discussing power projection from the homeland, with an emphasis on protection. Protection-focused opening remarks are delivered by General Glen D. VanHerck, commander of the U.S. Northern Command and the North American Aerospace Defense Command.

Nuclear Weapons Effects Simulation, Luis Palacios, Defense Threat Reduction Agency, 9 November 2022, <https://www.dvidshub.net/video/863746/nuclear-weapons-effect-simulation>. This is a Research and Development Nuclear Technologies Department, Defense Threat Reduction Agency-developed visualization video of the simulated effects of a 10-kiloton nuclear detonation against military units at various distances from ground zero. The video is intended only as a simulation to better aid warfighters in understanding what types of effects to expect after a low-yield nuclear detonation.

Protection (Strategic Landpower IRP PT 3), Jennifer Hunt et al., U.S. Army War College, Carlisle, Pennsylvania, 23 June 2023, <https://warroom.armywarcollege.edu/podcasts/23slirp-3/>. This podcast explores the potential role of the National Guard in strengthening cybersecurity defenses as a result of the rising prevalence of cyber threats. It also addresses the complexities of air and missile defense, which necessitate advanced technologies, strategic planning, and international cooperation. It concludes by highlighting the role of solid defense mechanisms in deterring potential aggressors, thereby preserving peace.

Critical Infrastructure Protection: Assessing the Risk in the Post Pandemic, Homeland Defense & Security Information Analysis Center, 15 September 2021, <https://hdiac.org/webinars/critical-infrastructure-protection-assessing-the-risk-in-the-post-pandemic/>. This webinar examines how the COVID-19 pandemic has posed new challenges for critical infrastructure protection, including the identification of decision makers and organizational responses to incidents. Many institutions are facing emerging threats and hazards as they return to regular operations, and this session reviews traditional and emerging risks and discusses the steps needed to safely manage the overall change in risk paradigm.

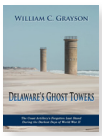
The Black Swan: The Impact of the Highly Improbable (2d edition)**,** Nassim Nicholas Taleb, Random House, 2010, ISBN 978-0-81297381-5. This update of the 2007 classic discusses risk, future planning, and the role of an almost infinite number of highly unlikely and unforeseen events—"a must read" for the protection planner.

United States Bomb Data Center (USBDC) Explosives Incident Report (EIR): 2022, U.S. Bomb Data Center, Huntsville, Alabama, 2022, <https://www.atf.gov/file/181946/download>. This short booklet reviews the 966 bombing incidents that occurred in the United States in 2022, and discusses bombing data for the last 5 years.

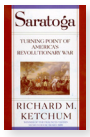
"The Maneuver Enhancement Brigade is the Support Area Command Post," *Military Review Online Exclusive***,** Colonel Patrick E. Proctor et al., U.S. Army , October 2018, <https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/Proctor-Barber.pdf>. The authors of this article underscore the significance of cybersecurity in modern defense architectures, asserting that as warfare increasingly shifts to the digital realm, robust cyberdefense measures are integral to ensuring national security. They advocate for continual innovation and upgrades of cybersecurity systems to counter evolving digital threats, effectively reinforcing defense mechanisms.

History

The Bay of Pigs, Howard Jones, Oxford University Press, 2008, ISBN 9780199743810. This is a dramatic account of the disastrous attempt to overthrow the prime minister of Cuba, Fidel Castro, in April 1961. Drawing on recently declassified Central Intelligence Agency documents, Jones deftly examines the train of self-deceptions and missteps that led to the invasion of U.S.-trained exiles at the Bay of Pigs. Ignoring warnings from the ambassador to Cuba, the Dwight D. Eisenhower presidential administration put in motion an operation that proved nearly unstoppable, even after the inauguration of John F. Kennedy. Meanwhile, both the Central Intelligence Agency and the Pentagon had voiced confidence in the outcome of the invasion.



Delaware's Ghost Towers: The Coast Artillery's Forgotten Last Stand During the Darkest Days of World War II (2d edition), William C. Grayson, AuthorHouse, 2005, ISBN 978-0-7414-4906-1. This short book explores how, when faced with depressed economic conditions prior to World War II, our Army responded to a new and revolutionary threat and goes on to describe how we protected a key section of our coastline throughout the war.



Saratoga: Turning Point of America's Revolutionary War**,** Richard M. Ketchum, Holt and Company, 1997, ISBN 978-0-712665025. In the summer of 1777, under General John Burgoyne, the British launched an invasion of America from Canada. It was the campaign that was supposed to crush the rebellion, but instead resulted in a series of battles that changed America's history and the history of the world.

Fiction

Ghost Fleet: A Novel of the Next World War, P.W. Singer and August Cole, Houghton Mifflin Harcourt, 2015, ISBN 978-0-544-70505-0. This very popular protection-heavy fictional novel has aged extremely well and is worth a reread, given today's latest international climate and developments.

Protection Writer's Guide

Protection is a professional-development bulletin designed to provide a forum for exchanging information and ideas within the Army protection community. We include articles by and about officers, warrant officers, noncommissioned officers, enlisted Soldiers, Department of the Army civilian employees, and others. Writers may discuss training, current operations and exercises, doctrine, equipment, history, personal viewpoints, or other areas of general interest. Articles may share good ideas and lessons learned or explore better ways of doing things.

Articles should be concise, straightforward, and in the active voice. If they contain attributable information or quotations, appropriate endnotes should be included. Text length should not exceed 2,000 words (about eight double-spaced pages). Shorter after action type articles and reviews of books on protection topics are also welcome.

Include photographs (with captions) and/or line diagrams that illustrate information in the article. Please do not include illustrations or photographs within the text; instead, send each of them as a separate file. Do not embed photographs in Microsoft® PowerPoint or Word. Save digital images at a resolution no lower than 200 dpi. Images copied from a website must be accompanied by copyright permission. Please see the Photo/Illustration Guide at <https://home.army.mil/wood/application/files/2516/5512/2839/Protection_Writers_Guide.pdf> for more information.

Provide a short paragraph that summarizes the content of the article and a short biography that includes your full name, rank, current unit, job title, and education; your mailing address; and a commercial daytime telephone number.

Articles submitted to *Protection* must be accompanied by a security release from the author's unit or activity security manager prior to publication; the security release cannot be signed by the author. All information contained in the article must be unclassified, nonsensitive, and releasable to the public. *Protection* is distributed to military units worldwide. As such, it is readily accessible to nongovernment or foreign individuals and organizations.

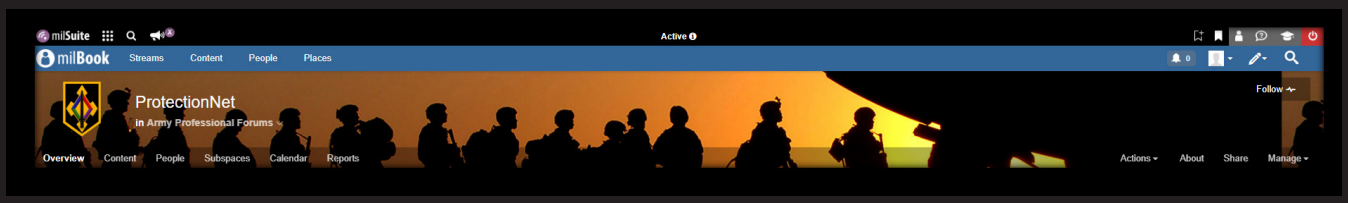
We cannot guarantee that we will publish all submitted articles, photographs, or illustrations. They are accepted for publication only after thorough review. If we plan to use your article in an upcoming issue, we will notify you. Therefore, it is important to keep us informed of changes in your e-mail address and telephone number. All articles accepted for publication are subject to grammatical and structural changes as well as editing for style.

Protection is published annually. Submission deadline for articles is 15 August. Send submissions in Word by e-mail to usarmy.leonardwood.mscoe.mbx.protectpb@army.mil.

Note: Please indicate if your manuscript is being considered for publication elsewhere. Due to the limited space per issue, we usually do not publish articles that have been accepted for publication at other Army venues.

Join ProtectionNET today!

https://www.milsuite.mil/book/community/spaces/apf/protectionnet



With access to ProtectionNet, authorized common access card (CAC) holders can —

- Share and request standard operating procedures.
- Stay connected to adjacent units.
- Influence future protection doctrine, concepts, and international agreements.
- Ask how others have solved a given challenge.

Bottom line: You are not alone!

PIN:215933-000