Protection

Professional Bulletin

2022 Annual Issue

HEADQUARTERS, DEPARTMENT OF THE ARMY
Approved for public release; distribution is unlimited.
PB 37-22-2

U.S. Army
Maneuver Support Center of Excellence
(573) XXX-XXXX
DSN 676-XXXX (563 prefix)

Commanding General
MG James E. Bonner **563-6166**
<james.e.bonner4.mil@army.mil>

FIELDED FORCE INTEGRATION DIRECTORATE (FFID)

Director, FFID
COL Mandi L. Bohrer **563-7244**
<mandi.l.bohrer.mil@army.mil>

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

Chief, Protection Division (Force Modernization Proponent), FFID
Mr. Barrett K. Parker **563-7105**
<barrett.k.parker.civ@army.mil>

CAPABILITIES DEVELOPMENT and INTEGRATION DIRECTORATE (CDID)

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

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

Chief, Maneuver Support Battle Lab
COL Joseph E. Elsner **563-6186**
<joseph.e.elsner2.mil@army.mil>

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

Chief, Concepts Division, Maneuver Support–CDID
COL James V. Rector **563-7955**
<james.v.rector.mil@army.mil>

MANEUVER SUPPORT CENTER OF EXCELLENCE HOMELAND DEFENSE/CIVIL SUPPORT OFFICE

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

Chief, Force Modernization
Mr. Brian J. Boston **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. The U.S. Army Maneuver Support Center of Excellence reserves the right to edit material. Articles may be reprinted if credit is given to the Maneuver Support Center of Excellence and the authors.

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.

Articles may be republished if credit is given to *Protection* and its authors. All photographs are official U.S. Army photographs unless otherwise noted. *Protection* reserves the right to edit material. *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>

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Acting Administrative Assistant
to the Secretary of the Army
2223005

DOCTRINE DIVISION, FFID

Chief, Doctrine Division
Mr. Les R. Hell **563-7332**
<leslie.r.hell.civ@army.mil>

Managing Editor
Ms. Diana K. Dean **563-4137**
<diana.k.dean.civ@army.mil>

Editor
Ms. Cheryl A. Nygaard **563-5226**
<cheryl.a.nygaard.civ@army.mil>

Graphic Designer
Mr. Dennis L. Schellingberger **563-5267**
<dennis.l.schellingberger.civ@army.mil>

Protection

Professional Bulletin

PB 37-22-2, 2022 Annual Issue

Maneuver Support Center of Excellence and Fort Leonard Wood Commanding General

Major General James E. Bonner

The entire team at the Maneuver Support Center of Excellence, Fort Leonard Wood, Missouri, is incredibly proud of the protection warfighting function community of practice. We want to thank you for your important and impactful efforts. You are a part of a tremendously diverse and unique team of professionals, and we appreciate your engagement—providing foundational input, relevant knowledge, and invaluable experiential lessons learned from across the force.

In the inaugural issue of *Protection*, I challenged you to provide a variety of viewpoints and to participate in professional dialog to evolve our capabilities across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) domains—and you delivered. Thank you. Your focused efforts allowed our work to progress in the following ways:

- Revising Army Doctrine Publication (ADP) 3-37, *Protection*.[1]
- Providing options for protection-related capabilities and forces.
- Piloting the Protection Integrator Course.
- Developing an additional skill identifier.
- Advocating for the Protection Decision Support Tool.
- Developing the All-Domain Protection Capabilities-Based Assessment through workshops and exercises.
- Integrating protection into experimentation, Army training exercises, and lessons learned.

Please continue to leverage our battle rhythm operational planning teams and warfighter forums to shape the Army protection capabilities. We appreciate your consistent participation in these activities and value your critical thought and focus. We also ask for your continued advocacy; please include protection in your unit activities, training meetings and exercises, and information-sharing forums and facilitate protection-related discussions within and outside of your formations.

Numerous avenues are available for generating dialog, from products (such as articles in this publication) to podcasts. Protection Net is one of several venues where the protection community can initiate conversations and share information regarding best practices, successes, and challenges. Protection Net, located on milSuite, is available at <https://www.milsuite.mil/book/community/spaces/apf/protectionnet>.

In this issue of *Protection*, you will find our first Protection Warfighting Function Professional Media List, which is intended to enhance individual and unit knowledge. We hope that you will make use of the list and that you will provide recommendations for additions.

Thank you for your participation, leadership, and contributions to the protection community. We are very proud to serve with you.

Endnote:

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

The All-Domain Protection Story

By Mr. Damon M. Yourchisin

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

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

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

The Problem

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

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

The Solution

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

- Enabling access in depth.
- Establishing and retaining dispersed support areas.
- Shaping movement corridors.
- Preserving essential capabilities (formations, assets, and activities).

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

Protection in MDO

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

Operational Environment Threats

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

Challenges

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

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

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

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

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

Experimentation Planning

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

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

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

Key Insights

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

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

Operationalizing protection and fully realizing the AFC Concept for Protection 2028[2] require that MSCoE assess the current state of protection across the WFF, develop new protection solutions, and educate the force. This work involves lead personnel from AFC and the U.S. Army Training and Doctrine Command as well as from across multiple proponents outside of MSCoE. Many aspects of current and ongoing doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) domain efforts operationalize the key protection concept themes of deny, enable, and preserve; some such aspects include—

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

(Continued on page 6)

The Protection Warfighting Function in Irregular Warfare

By Captain Emily A. Gasvoda

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

Background

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

Protection Cell

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

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

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

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

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

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

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

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

Endnotes:

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

[2]Ibid.

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

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

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

- **Protection materiel.** In driving forward to ensuring an MDO-capable force in 2030 and designing the force of 2040, there are three big MS-CDID/MSCoE ideas that could have an immediate effect:
  - Automation in breaching and chemical, biological, radiological, and nuclear hazard assessment needs to be fast-tracked.
  - Artificial intelligence support tools for synchronizing protection at echelons must be pursued.
  - The critical space where protection and deception intersect in offsetting vulnerabilities must be initially understood and exploited through next-generation obscuration.

Conclusion

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

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

Endnotes:

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

[2]Ibid.

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

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

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

Multi-Domain Operations:
The Latest Evolution of Operational Doctrine

By Captain Carlos J. Valencia

Doctrine represents the total collection of U.S. Army knowledge gained over 247 years of war, uneasy tensions, and peace. Over the past 40 years, the world and the operational environment (OE) in which we find ourselves have significantly changed, as various advancements have been made by peer threats. Loitering munitions, electronic warfare, unmanned systems, and nonnation state actors (among other technologies and factors) have revolutionized how war is now fought and how the Army must adapt to meet these threats. After a nearly 20-year focus on counterinsurgency operations, the Army began shifting its doctrinal focus back toward large-scale combat operations (LSCO) in 2017, with the publication of previous Field Manual (FM) 3-0, *Operations*.[1] Now, a 2022 edition of FM 3-0 introduces a new Army operational concept that retains the focus on LSCO, builds on the importance of integrating joint and multinational capabilities, and expands on the combined arms approach—with an emphasis on creating complementary and reinforcing effects with capabilities from multiple domains.[2]

Multi-domain operations (MDO) refers to the combined arms employment of capabilities from all domains that creates and exploits relative advantages to defeat enemy forces, achieve objectives, and consolidate gains during competition, crisis, and armed conflict. MDO constitute the Army contribution to the joint fight. All operations are MDO, regardless of joint force capabilities contributed at each Army echelon. This is because Army forces employ organic capabilities in multiple domains and continuously benefit from capabilities that they do not control; examples include benefits gained from the Global Positioning System and from combat aviation support from the U.S. Navy or the U.S. Air Force. MDO demand a mindset that focuses on how Army forces view the OE and threats. But what does the modern OE look like, and how do the domains fit in?

An OE is a composite of the conditions, circumstances, and influences that affect the employment of capabilities that bear on the commander's decisions. Within the context of an OE, a domain is a physically defined portion of the OE that requires a unique set of warfighting capabilities and skills. The OE includes portions of the land, maritime, air, space, and cyberspace domains as impacted through three dimensions (human, physical, and information). The land, maritime, air, and space domains are defined by their physical characteristics, and cyberspace—a manmade network of networks—connects them, as represented by the dots shown in Figure 1.

Leaders must understand how these three dimensions impact the OE. From a simple machine gun team crew action to a major offensive campaign, all operations affect the physical world, the humans who reside in it, and the information by which it is conceptualized. Additionally, MDO aim for Army leaders to think beyond previous planning considerations and emphasize the integration of the Army capabilities across the five domains in order to compound effects with sister Services and deter and defeat peer threats at the lowest cost.

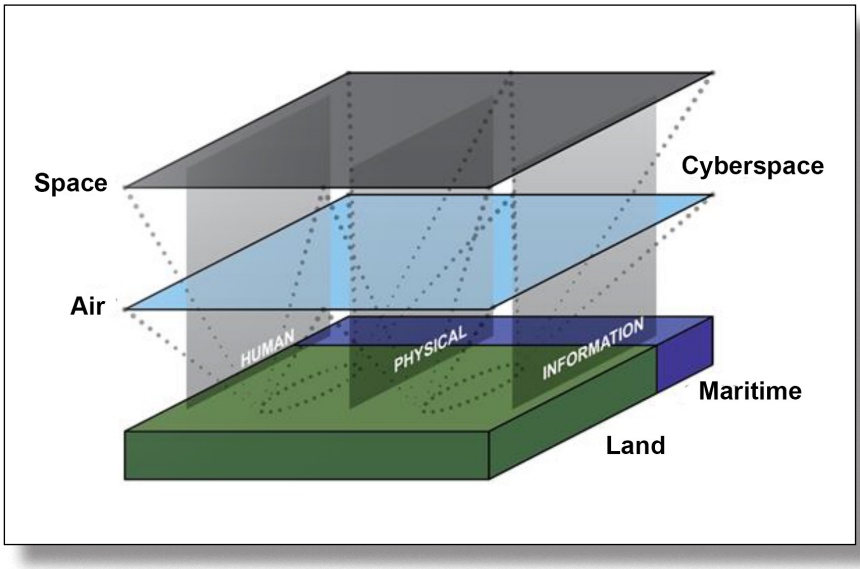


Figure 1. The OE

An additional change to the updated version of FM 3-0 is the introduction of the strategic situation, which stems from the competition continuum introduced in Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*.[3] The strategic situation describes how the Army conducts itself across the range of military operations in three strategic contexts—competition below armed conflict, crisis, and armed conflict. Together, these three strategic contexts form a progressive continuum along which the Army must be prepared to proceed in order to match an adversary's escalating violence and increases in U.S. national interest. In competition below armed conflict, nation or nonnation states with unaligned interests use various peaceful and malicious methods to compete with one another in order to gain an upper hand. The traditional Army contribution to unified action during this strategic context of competition below armed conflict consists of military engagement and security cooperation while preparing for armed conflict. As events or incidents that threaten U.S. national interests occur, the strategic context gradually moves toward crisis; this may require Army intervention, and Soldiers may be deployed to forward locations to deter conflict and prepare for war. If all else fails, then nation or nonnation states may begin using lethal force to achieve their goals; and in response, the Army conducts combat operations, exploiting its preparations from the competition and crisis strategic contexts to defeat the adversary. Competition below armed conflict, crisis, and armed conflict are not terribly foreign concepts, but the strategic situation helps leaders better conceptualize operations as the Army operates in different strategic contexts all across the world.

Along with the previously mentioned updates to FM 3-0, additional major updates and changes include—

- Establishing the dynamics of combat power—leadership, information, mobility, and survivability—which are generated by the warfighting functions.
- Identifying the four tenets of operations: agility, convergence, endurance, and depth. These tenets are attributes that should be built into all plans and operations, and they are directly related to how the Army operational concept should be employed. The new FM 3-0 introduces convergence as the concerted employment of capabilities from multiple domains against combinations of objectives to create effects against a system, formation, capability, or decision maker.
- Describing the nine imperatives as actions that Army forces must take to defeat peer enemy forces and succeed in operational environments extended through all domains.
- Providing an update to the operational framework. The update—
  - Expands assigned areas, introducing and defining zone and sector areas.
  - Removes consolidation area, as the consolidation of gains now occurs throughout the entire operation, regardless of location.
  - Reintroduces main effort, supporting effort, and reserve, which replace decisive, shaping, and supporting efforts.
- Adding informational considerations to the mission variables, which are aspects of the three dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information.
- Introducing influence as a ninth form of contact.
- Adding the theater strategic level as the fourth level of war.
- Adding chapters on Army operations in maritime-dominated environments and leadership during operations.

Similar to events of the past, the 2022 version of FM 3-0 will drive an evolutionary change across Army doctrine, including updates and changes to Army Doctrine Publication (ADP) 3-37, *Protection*,[4] and the family of associated publications that falls under the protection warfighting function—the warfighting function that enables the commanders to maintain force integrity and combat power through the integration of protection capabilities during competition below armed conflict, crisis, and armed conflict. Protection consists of the related tasks, systems, and methods that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action. As the Army doubles down on its focus on LSCO, FM 3-0 should serve as a reminder that protection results from many factors, including the protection warfighting function primary tasks, operations security, dispersion, deception, survivability measures, and the way in which forces conduct operations. Planning, preparing, executing, and assessing protection is a continuous and enduring activity.

Commanders and their staffs must understand the operational environment; be aware of their protection capabilities; and know how to coordinate, integrate, and synchronize protection capabilities to reduce risk, mitigate identified vulnerabilities, and create windows of opportunity throughout all Army operations. Emerging protection doctrine will raise additional questions and considerations for commanders, leaders, and staffs:

- How does the protection warfighting function complement and reinforce other warfighting functions and Service capabilities across each of the domains?
- How do the 16 primary protection tasks create effects through the different dimensions?
- How does the protection warfighting function contribute to competition below armed conflict, crisis, and armed conflict?
- How can protection measures prevent and mitigate disruptive effects that may occur while at unit home stations, at ports of embarkation, in transit to the theater, and upon arrival at ports of debarkation?
- How do commanders and staffs identify, prevent, and mitigate gaps and seams in the protection posture of friendly forces during LSCO?
- How does the Army prevent and mitigate enemy capabilities to conduct operations within the homeland, against power projection capabilities, in support areas, and into the deep maneuver and fires areas of the battlefield?
- How do commanders and staffs prioritize critical capabilities, assets, and activities?

Protection, which is not limited to a specific branch of the Army, is essential for preserving critical capabilities and mitigating risk across all domains. It will always be a key consideration when operating in multiple domains and during competition, crisis, and armed conflicted. Protection starts with each individual Soldier, but protection staffs must be forward-thinking, predicting hazards and threats that may not be readily apparent. Protection leaders must understand their place within the staff and must transcend from solely being subject matter experts in their particular field (policing, air defense, health services) to becoming protection experts. Without a comprehensive protection mindset, staffs may overlook risks to the force and open themselves up to the enemy ability to deny, degrade, or disrupt their advantages and limit their freedom of action. Protection staffs must embrace the protection principles (comprehensive, integrated, layered, redundant, and enduring) in order to contribute to the dynamics of combat power at the highest level. Only then will it be possible to complement other effects to deliver a powerful blow to the enemy and drive friendly momentum. If one warfighting function is lacking and does not synchronize with the others, a unit may lose its ability to enforce its will on the enemy.

The new FM 3-0 is a critical piece of doctrine that leaders must read in order to understand Army operations and the ways in which each warfighting function and every branch of the Army contribute to the fight. Protection doctrine will subsequently be updated and distributed throughout the Army for review. As drafts of the various publications begin to appear in e-mail inboxes, I implore each leader to read them and provide feedback; this is the only way that our doctrine can be improved.

Endnotes:

[1]FM 3-0, *Operations*, 10 June 2017 (now obsolete).

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

[3]JP 1, *Doctrine for the Armed Forces of the United States*, 12 July 2017.

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

Captain Valencia is a doctrine analyst/writer for the Military Police Branch, Doctrine Division, Fielded Force Integration Directorate, Maneuver Support Center of Excellence, Fort Leonard Wood, Missouri. He holds a bachelor's degree in history from the University of Texas, San Antonio.

EOD AND LSCO IN DOCTRINE

By Lieutenant Colonel Edward R. Runyan and Captain Stephen M. Hartman

As the Army continues to modernize to meet 21st Century challenges, recent examples in Europe help illustrate the need to prepare for large-scale combat operations (LSCO). During the past 2 decades of counterinsurgency operations (COIN) and low-intensity conflict, there has been an evolution of tactics that differ considerably from those used in the initial invasions of Iraq and Afghanistan.

What was old is now new, and what was new has now become old. While modern LSCO doctrine continues to evolve through lessons learned in the decisive-action training environment, functional capabilities such as explosive-ordnance disposal (EOD) continue to struggle in the transition of codifying doctrine from COIN to LSCO. While there is much debate within the EOD career field regarding how to best enable protection of forces and lethality in LSCO, the lack of definitive EOD LSCO doctrine continues to inhibit EOD inclusion in the decisive-action training environment. As with previous conflicts, this lack of inclusion creates unacceptable risk to combat operations, as EOD personnel cannot effectively posture to meet battlefield requirements, especially during initial entry into theater. Simply stated, the lack of definitive EOD LSCO doctrine continues to hinder inclusion of EOD at combat training centers (CTCs) and warfighter exercises (WFXs). The way forward hinges on understanding how EOD has enabled actions across the warfighting functions and how the capability continues to enable these actions in LSCO.

Just as in COIN, EOD personnel support unified land operations in LSCO by detecting, identifying, conducting on-site evaluation of, rendering safe, exploiting, and achieving final disposition of all explosive ordnance, including improvised explosive devices (IEDs) and weapons of mass destruction. Over the course of 21 years of fighting in a COIN environment, the employment of EOD capabilities largely became synonymous with combating IEDs. With the proliferation of IEDs as the enemy's primary weapon on the battlefield, the road-to-war training for EOD personnel, for good reason, centered on counter-IED operations.

This arguably further caused maneuver commanders to view EOD forces as IED experts, rather than as overall explosive-ordnance experts who were capable of supporting missions across the full range of military operations. This could have been the start of the problem, as core EOD skill sets across the conventional chemical and nuclear ordnance spectrum atrophied over time. As Army training is diligently refined to regain these EOD skills, codified EOD LSCO doctrine is essential in providing both EOD and maneuver commanders with a framework for establishing how EOD functional capabilities contribute to each warfighting function, to lethality, and to overall mission success.

An EOD Soldier participates in a team competition. Photograph credit: Staff Sergeant Apolonia L. Gaspar.

The EOD community must develop effective doctrine that concentrates on a starting point for command relationships, the roles of functional EOD commands at echelon, EOD core contributions to warfighting functions, and key EOD contributions to foundational tactical mission tasks. EOD forces are often directed to integrate with supported maneuver elements at CTCs and in WFXs. However, while integration is essential for every enabler on the battlefield, directing enablers to integrate suggests that it is incumbent on individual enablers to advocate for their capabilities (almost as salespeople) and that the success of the integration is solely dependent on how they articulate the value of their capabilities to the maneuver commander's mission success. EOD LSCO doctrine must serve as a framework for transitioning current EOD integration efforts (which are heavily reliant on self-promotion) to integration efforts that are predicated upon a doctrinal foundation. While mission

variables inevitably change over time, EOD LSCO doctrine must serve as a common point of departure, promoting initial shared understanding of EOD capabilities and initial integration success.

Given the Army functions in written foundational references such as Army doctrine publications, Army regulations, and operation orders, how can Army EOD leaders solidify an immediate initial LSCO doctrinal solution? Initially, at least, they should acknowledge that EOD LSCO doctrine will inevitably change over time. Therefore, it is more important to establish an imperfect starting point than to debate and delay a more perfect solution. While there have been multiple after action reviews and other products related to EOD unit experiences at CTCs and WFXs over the past several years, one of the more recent and successful examples stems from the 242d Ordnance Battalion (EOD), Fort Carson, Colorado, experiences in support of the California National Guard 40th Infantry Division (40ID), Los Alamitos, California, during WFX 22-04. The experiences of the 242d Ordnance Battalion may help to serve as an imperfect starting point.

Upfront, the 242d Ordnance Battalion and 40ID were not designated training audiences for WFX 22-04. Throughout the training leading up to and during WFX 22-04, 40ID remained exceptionally receptive to 242d Ordnance Battalion training objectives. As a division enabler, the 242d Ordnance Battalion remained under the operational control of 40ID throughout the exercise, with direct coordination authorized to the 52d Ordnance Group (EOD), Fort Campbell, Kentucky, which served as the theater level EOD command. According to the 242d Ordnance Battalion after action reviews, this relationship allowed the 242d to understand and synchronize with the theater level EOD common operating picture. Through the 40ID rear-area command post, the 242d used the protection warfighting function as a main conduit for influencing actions across the other warfighting functions. The 242d Ordnance Battalion commander remained the senior EOD advisor to the 40ID and retained the ability to move and posture subordinate EOD companies across the 40ID close and rear areas in order to meet current and projected EOD requirements. While other CTC and WFX after action reviews outline how supported units have delegated command relationships to units commonly referred to as "pockets for enablers" (such as maneuver enhancement brigades and brigade engineer battalions), the 242d remained in direct operational control of 40ID. This allowed the 242d to establish a division level EOD common operating picture and inform 40ID about how residual battlefield enemy and friendly explosive ordnance might impact future combat operations as the division deep area transitions to the division close area and the close area transitions to the division rear area.

While the 242d Ordnance Battalion experience may not be a perfect example, it can serve as viable doctrinal starting point. Three main takeaways may, at a minimum, help establish a foundational understanding of the EOD battalion role at the division level. First, the 242d Ordnance

An EOD officer works a lane in a bomb suit during a multi-Service competition. Photograph credit: Staff Sergeant Apolonia L. Gaspar.

Battalion remained in operational control of the division throughout all phases of the exercise, enabling the 242d to support division operations across the deep, close, and rear areas. Second, the 242d commander retained the ability to posture exceptionally limited EOD capabilities to best meet collective division requirements; this was particularly vital given the limited quantity of EOD capabilities in the exercise theater. Third, through the rear-area command post, the 242d remained a key operational contributor, advising the 40ID on battlefield explosive-ordnance risk and providing viable mitigation strategies. This demonstrated the role that EOD plays in enabling lethality. By starting with EOD battalion LSCO doctrine and then using these takeaways, Army EOD personnel may help further develop doctrine at echelons above and below the division. This would also help array and posture limited EOD capabilities to support the most likely tactical mission tasks at the brigade echelon and below.

With the manning reductions currently underway at EOD battalion and ordnance group headquarters, doctrinal development is even more imperative. As in COIN, the need for EOD across the deep, close, and rear areas at each echelon is abundant and critical. We ask that the Army publish doctrine that clearly defines how EOD enables lethality and mission success without waiting for unanimous consent. We further request the establishment of a common framework for EOD company and battalion level leaders to follow and, in the process, the creation of a road map to prepare EOD Soldiers to better support LSCO.

Lieutenant Colonel Runyan is an EOD officer who commanded the 242d Ordnance Battalion (EOD) from July 2020 to July 2022. He holds a master's degree in military art and science from the Command and General Staff College, Fort Leavenworth, Kansas.

Captain Hartman is the operations officer in charge at the 71st Ordnance Group, Fort Carson. He holds a bachelor's degree in biology from Crown College, St. Bonifacius, Minnesota.

Where Did the IEDs Go? Thoughts on Strategic and Operational Rear Areas

By Mr. William C. Dahms

"It is a myth that military organizations tend to do badly in each new war because they have studied too closely the last one; nothing could be farther from the truth. The fact is that military organizations, for the most part, study what makes them feel comfortable about themselves, not the uncongenial lessons of past conflicts. The result is that often militaries must relearn in combat and usually at a heavy cost; lessons that were readily apparent at the end of the last conflict."

—Williamson Murray[1]

During Operation Desert Shield/Storm in the early 1990s, the U.S. Army was unquestionably at its highest level of readiness. During the ensuing years leading up to 11 September 2001, Army forces gradually lost their overmatch advantage. That was a time of tranquil chaos. Our adversaries continued to examine our capabilities, attempting to better understand the magnitude and reach of our combat power. As a result, these adversaries began to formulate alternative means to threaten America. It was then that the world changed and a new era of threats that were not restrained by the previous global wars of World War I and World War II emerged. Improvised explosive devices (IEDs)—which, according to the National Security Strategy,[2] are one of the oldest forms of weapons that can be employed against any superior force—became the weapon of choice for the enemy against the United States in Iraq, Afghanistan, and South America. Our experience with IEDs and other explosive hazards (EH) had been limited to the Vietnam War and World War II.[3, 4, 5, 6]

History tends to repeat itself. For example, the recent Russian incursion into Ukraine was preceded by the Russian invasion of Crimea in 2014. However, with a return to large-scale combat operations (LSCO) and the advent of multi-domain operations, the next conflict obviously will not be like those of last 2 decades. Although our adversaries will likely continue to employ IED capabilities, they will improve their effectiveness through the use of unmanned aerial vehicles for gathering intelligence, performing surveillance, conducting reconnaissance, and delivering lethal payloads. When coupled with more advanced robotics, autonomous platforms, artificial intelligence, and cyber/electromagnetic warfare operations, the protection challenge will be significant.

Our peer adversaries have already revealed how they intend to challenge us. They have created multiple layers of defensive standoff through their antiaccess and area denial systems. U.S. forces have superior weapons—maybe not in quantity, but in quality and reliability. The training proficiency and skill of U.S. forces are also superior. But what about our most vulnerable support areas, where there are fewer tactical units?

The solution to this issue most likely lies in the shaping of the environment, through the calibration of our forces, and the degree to which unified action partners are integrated. Protection, like any other response to a threat including IEDs/explosive hazards (EHs) is not a linear activity. It is dependent upon our ability to plan, prepare, execute, and assess our protective posture in a continuous and enduring manner. The key to success is sustaining a balanced protected support area, layered by depth, and an echelon enabled with speed and sufficient combat power while maintaining a high operational tempo.

Responsive and mobile sustainment must also keep pace with maneuver forces over extended distances. Let's set aside the discussion of tactical forces in our support areas and Threat Level I, II, and III concerns for a moment and focus upon the obstacles to our freedom of movement that we are most likely to face in our support areas. Let's focus on IEDs and EHs like unexploded ordnance, conventional mines, explosive booby traps, and explosive remnants of war in the battlespace. IEDs were unquestionably a challenge over the last 2 decades, and there is no clear indication that their use will be discontinued in future conflicts. IED attacks still occur daily, both abroad and in the homeland—yet, the terms IED and EH are mentioned only one time each in Army Doctrine Publication (ADP) 3-37, *Protection*.[7]; the likelihood that EH will be encountered along routes is implied—but not specified—within the terms of area security and routes. So, what are we missing? We're missing the capacity for EH mitigation in our support areas and its integration into our area security activities.

Our strategic and operational support areas are vulnerable in a way that is similar to the vulnerabilities of our supply convoys of World War II. According to the March 2006 *Defense Science Board Report*, "When there are no front lines, all forces are at risk and logistics convoys, like merchant ship convoys of World War II, become 'movements to contact' or are targets for loosely organized enemy actions."[8]

"Many EH attacks may not be traditionally adversarial in nature (as when we are not at war) but tend to be more criminally or politically motivated and are reported with frequency."

Many IED/EH employments may not be traditionally adversarial in nature (as when we are not at war) but tend to be more criminally or politically motivated and are reported with frequency. It is clear that our strategic and operational rear areas or support areas will continue to be vulnerable.

Lucrative locations, such as those containing transportation hubs, power or electrical substations, water supplies, sewage systems, administrative facilities, infrastructure, communications equipment, and religious convergencies will remain soft targets. This vulnerability affects our ability to project power and to sustain force tactical operations. In the past, we focused upon the effects to tactical operations. We now need to consider expanding the threat environment to include our support areas. Events in Ukraine serve as a recent example of how a combination of IEDs and technology can be employed against a superior force in order to delay, disrupt, deter, and deny operations and command and control. Other examples include the fighting in Crimea in 2014 and the little-known Karabakh War of 2020 between Azerbaijan and Armenia. A key theme of recent and historical events is clear: It is essential to have consistent sustainment flow to forward support areas in order to maintain offensive momentum.

During the February 2022 Maneuver Conference at Fort Benning, Georgia, 1st Cavalry Division leaders provided an insightful review of how they intend to initially fight in a LSCO environment. The vulnerabilities of our support areas were specifically called out during this conference. Operations in Crimea in 2014, Azerbaijan in 2020, and Ukraine in 2022 have made it clear that mines, IEDs, and other EH will remain a part of the future battlefield; where and how these explosives are used are what we need to prepare for now. It is clear that, for successful operations, the Penetration Division requires a protection brigade and substantial reinforcements. This includes an engineer brigade just to mitigate risks associated with gap crossings (LSCO Gap 8) to set conditions for operational success. The general nature of a heavy-division fight is as a high-risk/high-reward operation. U.S. Marine Corps leaders are also advocating for the reestablishment of counter-improvised explosive device (C-IED) programs and training before deployments.[9] Naturally, commanders are in favor of risk reduction and advocate for what their experiences have shown to be effective ends-ways-means risk. Risk mitigation and force structure/budgetary restrictions are two parts of the Army and Marine Corps challenge. The ability to balance threats against force structure with the reality of our budget and manpower limitations will remain a significant challenge to both Services.

When considering how EH may be viewed on the future battlefield in the context of protection, some specific questions come to mind. We have an opportunity to address identified shortfalls, while preparing the best we can for future conflicts. With some modifications, the protection brigade for EH operations is needed to augment LSCO operations. To that end, the following thought-provoking questions should be asked and addressed:

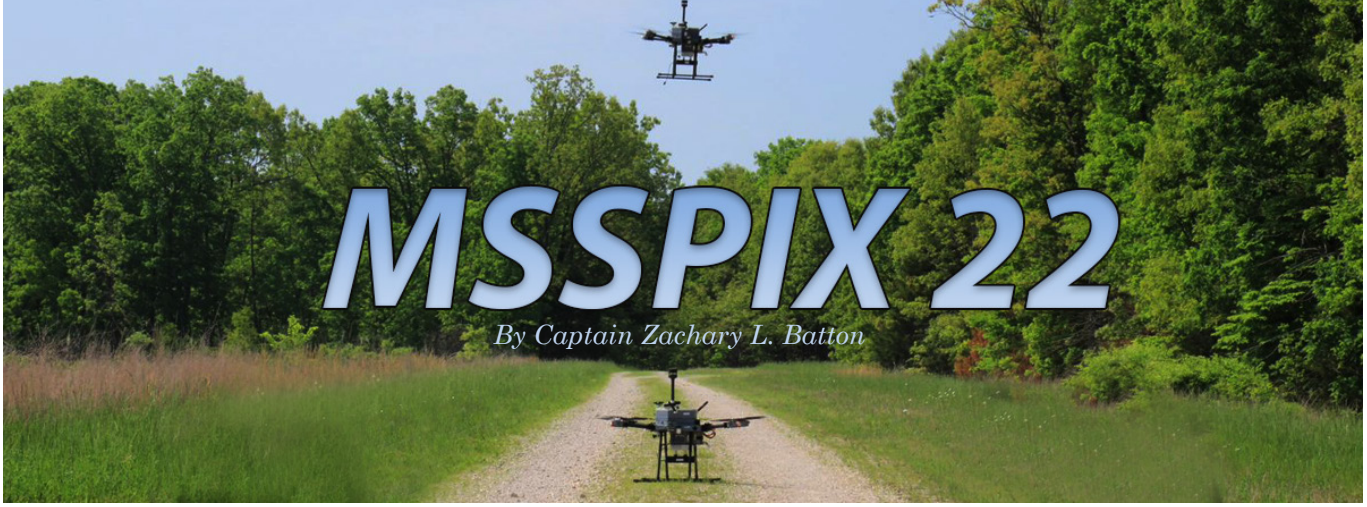
- Has the Army adequately designed the protection brigade to conduct C-IED operations for corps and divisions?
- Does the Army have enough capacity to mitigate the effects of EH in our support areas in terms of route clearance companies, explosive-ordnance disposal, engineer brigades/battalions, or EH coordination cells or organizations?
- How would adversaries most likely employ IEDs during LSCO?
- Is the United States adequately training Soldiers and combined arms formations to mitigate the effects of EH in support areas?
- Where can commanders receive attack-the-network/network engagement, military search, and site-exploitation training?
- Will military search (intermediate and advanced) and site exploitation operations be needed?

Fortunately, the purpose of the Counter Explosive Hazards Center (CEHC), Fort Leonard Wood, Missouri, is to preserve the fighting force by providing EH awareness to deploying forces, assisting in identifying and fielding viable countermeasure solutions and technologies, and developing the intellectual and situational superiority of combat units. CEHC also collects, analyzes, and stores C-IED/EH information in such a manner as to allow easy access by warfighters. The repository is aligned with the current U.S. Army "C-IED Strategy Lines of Effort."[10] Each line of effort is organized with knowledge from past conflicts and a mix of historical, current, and technical resources. Community resources for C-IED/EH Army professionals are available at: <https://www.milsuite.mil/book/community/spaces/apf/counter-ied> (common access card-enabled/protected).

Endnotes:

[1]Williamson Murray, "Thinking about Innovation," *Naval College Review*, Vol. 54, Issue 2, 2001, <https://digital-commons.usnwc.edu/nwc-review/vol54/iss2/11>, accessed on 9 September 2022.

(Continued on page 15)



MSSPIX 22

By Captain Zachary L. Batton

The Maneuver Support Battle Laboratory, Fort Leonard Wood, Missouri, and the Sustainment Battle Laboratory, Fort Lee, Virginia, annually execute the Maneuver Support Sustainment and Protection Integration Experiment (MSSPIX) under the oversight of the U.S. Army Joint Modernization Command, Fort Bliss, Texas. MSSPIX is one of four Army focused warfighter experiments funded by the Futures and Concepts Center, U.S. Army Futures Command, Fort Eustis, Virginia; it focuses on sustainment- and protection-based capability gaps, using emerging prototype technologies and capabilities developed by government laboratories and private industry.

During the annual experiments, Soldiers have the opportunity to use prototype systems in an operationally relevant environment. In return, technology developers receive Soldier feedback and some insight into Army priorities. This year, MSSPIX 22 was executed at Fort Leonard Wood and Fort Lee from 2 to 17 May 2022. With the help of 27 Soldiers tasked from four U.S. Army Forces Command installations, the Maneuver Support Battle Laboratory assessed the potential for using emerging technologies to address existing capability gaps and to provide input for capability development documents. This article highlights some of the technologies that were assessed during MSSPIX 22 and describes the focus of each of those assessments.

The Mobile-Acquisition Cue and Effector System©, developed by Northup Grumman, is an air defense vehicle that is fitted with a 30-millimeter M230LF Bushmaster cannon, incorporated with an automated targeting platform. The Mobile-Acquisition Cue and Effector System can successfully detect, identify, track, and eliminate unmanned aircraft systems (UASs). The platform is designed to provide on-the-halt capability, nondedicated air defense, and ground detection to units on the move. During the MSSPIX 22 event, military police and infantry Soldiers were trained on the use of the targeting and detection system incorporated into the technology and multiple live-fire scenarios were conducted to demonstrate the capability of the system to engage fixed-wing and rotary-wing UASs.

The Anduril Lattice© family of systems was also tested during MSSPIX 22. It is unique in that it combines surveillance capabilities with an artificial-intelligence-enabled Lattice software platform. Radar and sensors, along with the artificial-intelligence-enabled software, presents prioritized threat alerts to Soldiers, reducing the cognitive load on operators while providing an autonomous reconnaissance capability via the use of a rotary-wing UAS platform. The advanced sensors can also be used to gather detailed targeting information about potential threats. The Lattice software is designed to elevate situational awareness and provide Soldiers with additional planning time to coordinate denial activities.

A Soldier receives instruction on the Mobile-Acquisition Cue and Effector System.

The Joint Program Executive Office for Chemical, Biological, Radiological, and Nuclear (CBRN) Defense has developed CBRN sensors in robotic platform technology, which provides detection, identification, and mapping of weapons of mass destruction hazards via its modular detection payloads attached to a UAS. The software includes chemical plume prediction and radiation heat-mapping capabilities that help mitigate exposure risk to personnel and equipment by maximizing standoff distances during CBRN reconnaissance. During MSPIX 22, CBRN Soldiers were trained on the detailed mission setup and deployment of the autonomous UAS platform and scenarios that included a live radiation source and a simulated chemical plume (which demonstrated the ability of the system to conduct CBRN reconnaissance at standoff) were conducted.

The InstantEye© UAS, developed by InstantEye Robotics, is a small, lightweight, autonomous UAS designed to be rapidly deployed by any Soldier to conduct tactical close-area reconnaissance or deploy light payloads. The compact InstantEye fits into a standard Army pack,

Training on an InstantEye UAS with attached payload

which allows the Soldier to deploy it while on mission. During MSSPIX 22, the system was used by a mix of military police, engineer, and infantry Soldiers to demonstrate its minimal training burden and its reconnaissance capabilities against personnel, vehicles, and areas of interest under operational scenarios. The ability of the system to deploy a reconnaissance robot into a facility of interest was also demonstrated during MSSPIX 22.

Finally, during MSSPIX 22, the U.S. Army CBRN School, Fort Leonard Wood, assessed four different technologies designed to provide personnel-carried detection of chemical vapors and provide users with alerts of a suite of chemical agents at greater sensitivity and lower false-alarm rates than those of existing Army systems. These technologies, referred to as compact vapor chemical agent detectors, were developed by N5 Sensors©, GE Research©, Teledyne FLIR©, and Collins Aerospace©. The focus of the assessments was to determine the burden on the warfighter payload and any interference with Soldiers' primary mission. All vendor-presented devices were compact and lightweight and could be strapped or clipped onto the Soldiers. CBRN and infantry Soldiers compared the variants of the compact vapor chemical agent detectors and provided feedback on the device interfaces, functional controls, and control limitations that could be assessed while in personal protective equipment.

The assessment of emerging prototype systems is an important component of the capability development process. Capability developers learn about the latest state-of-the-art advancements and how new technologies may be able to fill capability gaps in order to better define key performance parameters and system attributes, leading to more-refined requirements and improved capability development documents. At the same time, science and technology developers receive crucial feedback from military users, which helps ensure that the new systems are not only relevant but also operationally useful. Army focused warfighter experimentation events play a critical role in Army modernization by providing a learning venue where military problems and potential solutions in a multi-domain operations-relevant environment may be better understood.

Captain Batton is the experimentation officer for the Maneuver Support Battle Laboratory, Fort Leonard Wood. He holds a bachelor's degree in physical education from the University of North Carolina, Pembroke.

("Where Did All the IEDs Go? . . . ," continued from page 13)

[2]*Standing Well Back* website, <https:\\standingwellback.com>, accessed on 1 September 2022.

[3]Glenn K. Otis, "Threat to the Rear: Real or Myth?" Land Warfare Paper No. 2, Association of the U.S. Army, November 1989, <https://www.ausa.org/sites/default/files/LWP-2-Threat-to-the-Rear-Real-or-Myth.pdf>, accessed on 2 September 2022.

[4]Mark Gilchrist, "Reconsidering Rear Area Security—The 101st Airborne Experience During Operation Market Garden," *The Strategy Bridge*, 17 September 2017, <https://thestrategybridge.org/the-bridge/2017/9/17/reconsidering-rear-area-security>, accessed on 1 September 2022.

[5]Lester Grau and Charles Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces*, Foreign Military Studies Office, Fort Leavenworth, Kansas, 2016.

[6]Marc Tranchemontagne, "The Enduring IED Problem: Why We Need Doctrine," *Joint Force Quarterly 80*, 1st quarter, 2016, <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643235/the-enduring-ied-problem-why-we-need-doctrine/>, accessed on 1 September 2022.

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

[8]*Defense Science Board Report*, March 2006, <https//dsb.cto.mil>, accessed on 9 September 2022.

[9]Marine Corps Order (MCO) 3502.10, *Counter-Improvised Explosive Device Training and Education Program*, 11 December 2018, <https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1714284/mco-350210/>, accessed on 9 September 2022.

[10]"C-IED Strategy Lines of Effort," U.S. Army, 2022, <https://www.milsuite.mil/book/community/spaces/apf/counter-ied>, accessed on 9 September 2022.

Mr. Dahms is a retired U.S. Army engineer and Functional Area 50 force manager. He holds a bachelor's degree in geography from the University of Wisconsin, Oshkosh, and a master's degree in security management from Webster University. He is a contractor in support of the Strategic Support Division, CEHC, U.S. Army Engineer School, Fort Leonard Wood.

Integrating Protection Into Modern-Day Wargaming

By Major Shawntria M. Mosley and Captain Justin N. Lassond

The U.S. Army has transitioned from 20 years of concentrating on counterinsurgency operations to focusing on large-scale combat. In an effort to "shake off the dust," the Army has turned to wargaming as a method of making the rapid modernization changes needed for the United States to succeed in the future operational environment. This article describes what wargaming is and is not, the modernization of wargaming and why the Army chose the Operational Wargaming System (OWS) as its medium, and strengths and limitations of the OWS as it relates to the integration of protection into the game.

Wargaming

The Army is not new to wargaming. The first known use of wargaming in the Army was in 1867,[1] and the practice has been used in various capacities ever since. Wargaming is a tool that enables players the ability to experiment and then analyze the outcomes that transpire, while also revealing associated risks. Wargaming is not magic, nor does it serve as a crystal ball that holds all the answers; nevertheless, if used correctly, it can be powerful.

Three main components are integral to wargaming: the blue force, the red force, and the white cell. The blue force represents friendly forces, the red force represents the adversary and its supporters, and the white cell represents adjudication. The red and blue forces are molded to represent the capabilities of their formations and their placement in the operational environment. Analysts spend hours analyzing each assumed outcome and extracting conclusions to determine the most probable path to victory.

Possibly the greatest challenge of wargaming is understanding what it is and what it is not. A wargame is not a simulation. Rather, it is a tool meant to invite thoughts and discussion. Wargaming has evolved since its introduction but has remained true to its roots. It gives users a peek into what could happen so that decisions can then be made to mold the outcome.

Modernization of Wargaming

The Army is constantly modernizing and developing capabilities; therefore, wargaming must also undergo development. Modern-day wargaming has been developed through a more scientific approach by adopting concepts of the scientific method. The scientific method refers to a procedure consisting of systematic observation, measurement, and experiment and the formulation, testing, and modification of hypotheses that support a scientific theory.[2] The supporting Army framework is called the Strategic Cycle or the Caffrey Loop (see Figure 1).[3] Whithin this framework, history is moved into theory, theory into doctrine, doctrine into plan, and plan into execution. Wargaming is the execution tenet in this framework. The outputs from the execution or wargame are added to history, and the cycle is repeated. Ultimately, the supported hypotheses become educated guesses that enable the Army to play out future conflict without participating in an actual conflict.

As the Army transitions to multi-domain operations (MDO), the integration of electronic warfare and space operations contributes to armed forces fighting on a more transparent battlefield, where the adversary can track in real time. It is anticipated that by the year 2040, the battlefield will be fully transparent due to an increase in the number and availability of technological advancements worldwide. The addition of new domains in an ever-changing operational environment brings new challenges. MDO serves as the Army's operating concept for countering and defeating near-peer to peer adversaries; the need for unified effort among joint forces in overcoming MDO challenges is a common theme. For the past 2 decades, military operations have focused on counterinsurgency. Today, the transition to MDO is driven by global threats from modernized Russian and Chinese forces, which have studied and learned from observing U.S. conflicts in Afghanistan and Iraq. As a result, the United States is in drastic need of innovation to keep pace with its adversaries and remain a competitive superpower. The U.S. Army Futures Command is using wargames as one means of fulfilling its role in modernizing the Army to meet operational challenges. Wargaming enables Army senior leaders to make the best decisions for prioritizing modernization efforts that will impact both the investment and innovation trajectories and make U.S. forces competitive and successful in future conflicts. To meet the need for innovation while also addressing the need for optimal synchronization of the joint force, the Army Futures Command has

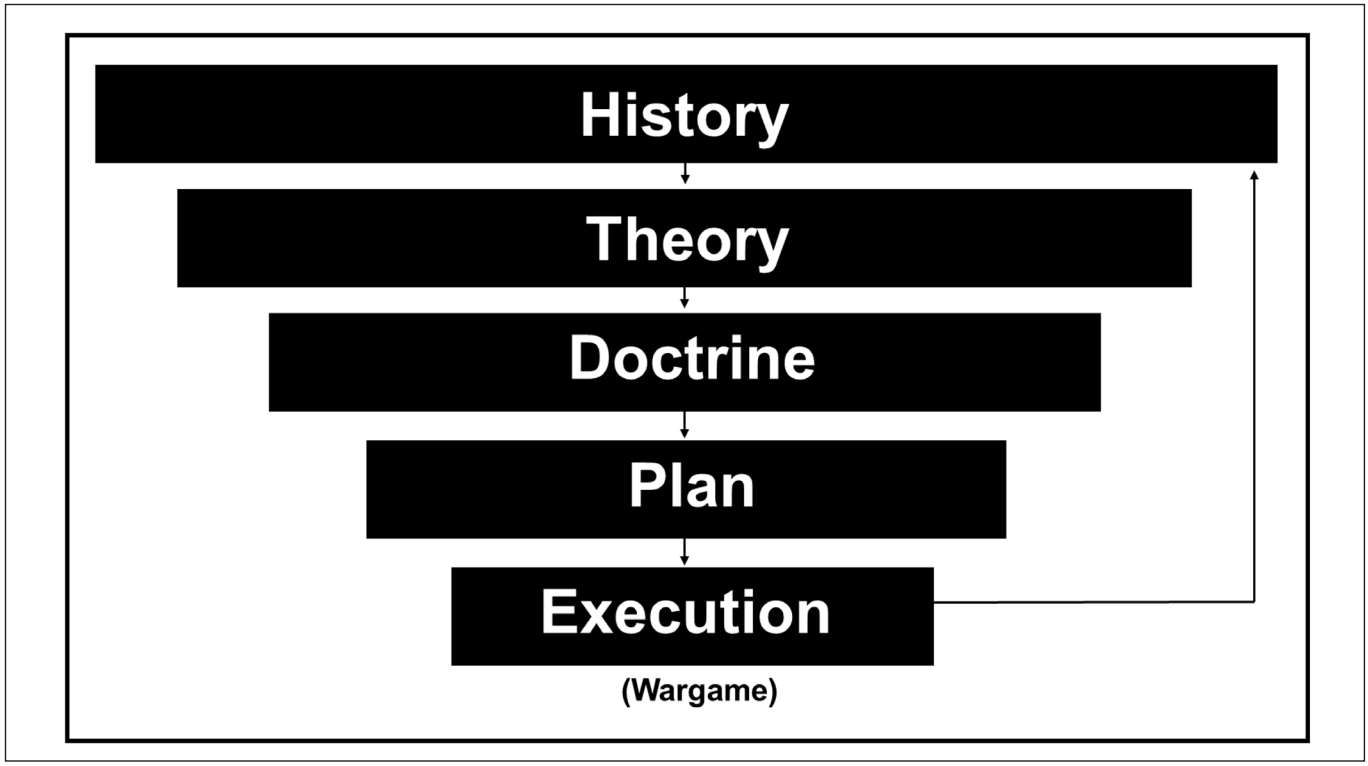


Figure 1. The Caffrey Loop

adopted the use of OWS. OWS is a turn-based strategy game that includes red- and blue-force and white-cell structure, transitioning a traditional tabletop experiment into a computerized flexible and adaptable digital simulation environment.

OWS Strengths and Limitations

An effective wargame design must accomplish two things: It must capture meaningful analysis, and it must minimize overencumbered game design details. One of the strengths of OWS is that it allows for the integration of joint forces across all domains; it is not maneuver-centric, as it rewards convergence of all warfighting functions. One of the limitations of OWS is that it does not naturally allow for the fidelity of unit capabilities at lower echelons. OWS encompasses brigade and higher-level inner workings in a given operational environment and focuses on divisions as the unit of action. With significant Army capabilities embedded at lower echelons, the wargaming community faces a significant challenge when designing a system to account for modernization at every echelon. The Concepts Division, Maneuver Support–Capabilities Development and Integration Directorate, Fort Leonard Wood, Missouri, in coordination with the Futures and Concepts Center, U.S. Army Futures Command, Austin, Texas, determines maneuver support protection requirements and creates ways to integrate the corresponding capabilities into OWS.

Integrating protection; engineer; military police; and chemical, biological, radiological, nuclear capabilities into OWS is not an easy endeavor since each branch has unique requirements. However, it is imperative that the wargame be designed as accurately as possible in order to refine analyses of future capability sets. As an example, one effect that engineers play with within OWS is terrain-shaping obstacles (TSO). TSO are best represented as close, mid, and deep (see Figure 2, page 18). For close TSO, as the game progresses, a "fortification bonus" is added to decrease the likelihood of successful attacks by the red force, thereby providing increased protection/survivability of the blue force. It is assumed that the future means of delivery (rocket, air, or tube) of antitank mines used for TSO will be highly accurate; therefore, mid/deep TSO will not be limited by the accuracy of placement of the munition—but rather, by the number of munitions available or the magazine depth. Once a mid/deep TSO is placed on the physical game board, there is a 50 percent chance of its success; and if successful, enemy movement will be reduced by 50 percent.

Rules of war and international policies agreed to by the United States apply in OWS. TSO activities require overwatch, and overwatch requires resources. Therefore, additional overwatch resources must be considered and necessary resources must be applied. However, because the Army has only so much overwatch capability, the use of a TSO could result in the constraint of important resources that are necessary for other mission requirements. This illustrates the need for the Department of Defense to synchronize and execute joint operations. The traditional Army method of self-reliance creates potential vulnerabilities that can be

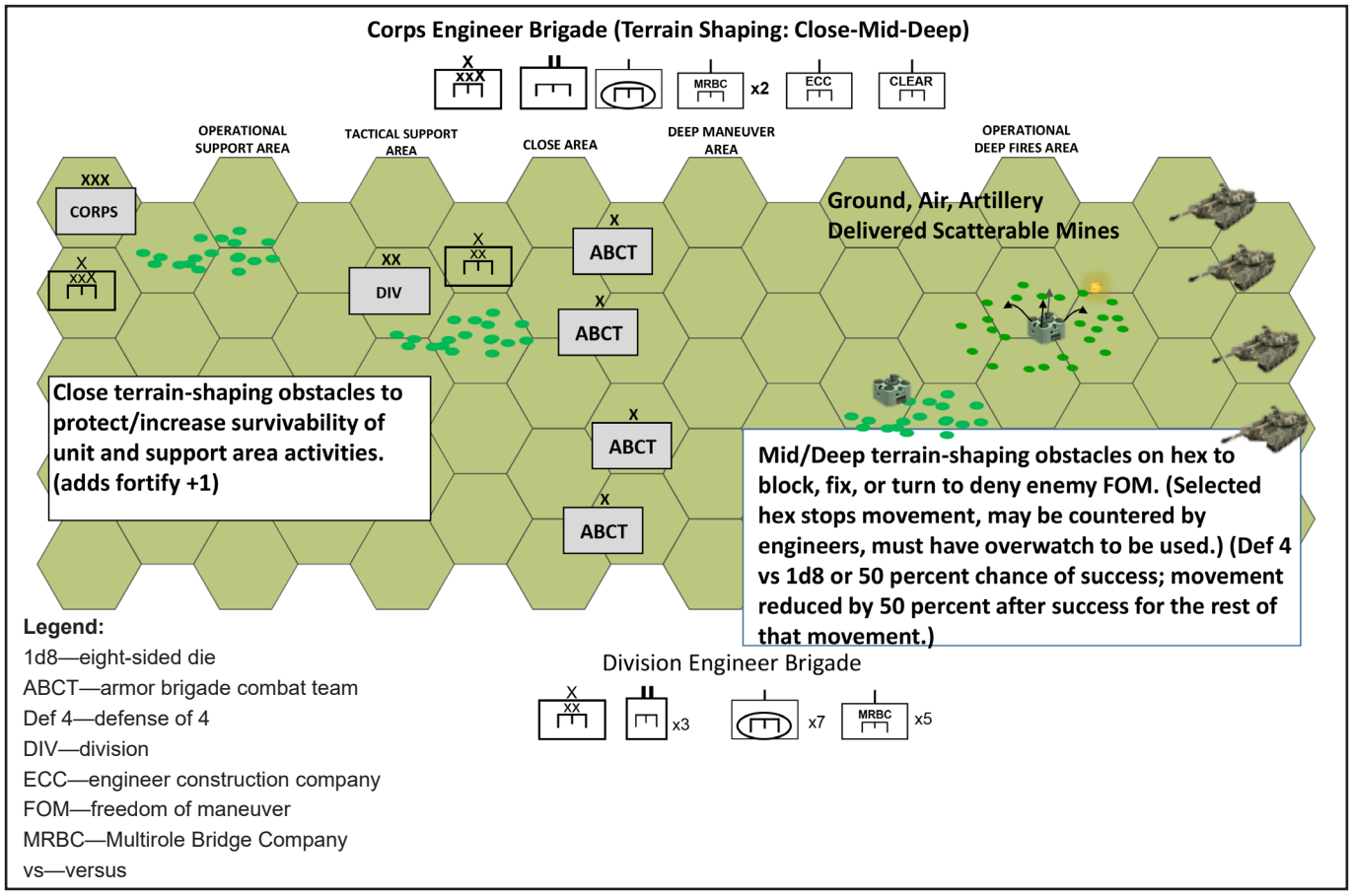


Figure 2. Close, Mid, and Deep TSO

exploited by the enemy. The probability of success in the future operational environment hinges on the synchronization of resources and capabilities, with a more collective joint approach.

Once concepts are played out in a wargame, additional analysis is completed in order to refine capability thresholds as concepts move toward requirements. It is important to view OWS as an ever-evolving, malleable gaming system in which thoughts and processes are refined. If used correctly, OWS—or any wargaming system, for that matter—offers significant returns at low cost. As new concepts are created, new testing baselines are established and the Caffrey Loop begins again. The key to wargaming is not to produce a better analysis; rather, it is to transform a given analysis into information that cannot be ignored. Time, money, resources, and lives can all be saved as we journey through the uncertainty of the future.

Conclusion

As the Army commits to force innovation, wargaming is one tool that can be used to make the best-educated investments for change in the future. The adoption of OWS allows for the Army to experiment with a joint force perspective that is imperative for success in the future operational environment. Protection is key in order for the United States to succeed in conflicts against its peers. Maneuver Support—Capabilities Development and Integration Directorate and OWS communities are committed to ensuring future success by integrating all domains of protection into the Army innovation initiative.

Endnotes:

[1]Farrand Sayre, *Map Maneuvers and Tactical Rides*, Springfield, Massachusetts, 1911, p. 22.

[2]"Scientific Method," *Lexico*, <https://www.lexico.com/en/definition/scientific_method>, accessed on 12 August 2022.

[3]Matthew B. Caffrey, "On Wargaming: How Wargames Have Shaped History and How They May Shape the Future," *Naval War College Newport Papers*, 2019, p. 6.

Major Mosley is the chief of the Chemical, Biological, Radiological, and Nuclear Branch; Concepts Division; Capabilities Development and Integration Directorate; U.S. Army Futures Command; Maneuver Support Center of Excellence; Fort Leonard Wood. She holds a bachelor's degree in biology from the University of Maryland Eastern Shore, Princess Anne; a master's degree in information systems from the Naval Postgraduate School, Monterey, California; and a doctor of chiropractic degree from Sherman College of Chiropractic, Boiling Springs, South Carolina.

Captain Lassond serves as projects officer for the Chemical, Biological, Radiological, and Nuclear Branch; Concepts Division; Capabilities Development and Integration Directorate; U.S. Army Futures Command; Maneuver Support Center of Excellence. He holds a bachelor's degree in financial economics from Brigham Young University–Idaho, Rexburg.

By Chief Warrant Officer Three Macio E. Brown

"Technology cannot advance without the vision of a better tomorrow"
—Chief Warrant Officer Three Macio E. Brown

The Chemical Biological Operational Analysis (CBOA) event, developed and executed by the Defense Threat Reduction Agency (DTRA), provides researchers an opportunity to elicit warfighter feedback during the technology development process of emerging chemical, biological, radiological, and nuclear (CBRN) capabilities for use in a realistic operational environment.

CBOA 22 was held at Eglin Air Force Base, Florida, in May 2022. In its role as the Joint Science and Technology Office (JSTO) for the Chemical and Biological Defense Program, Chemical and Biological Technologies Department, DTRA, is the Department of Defense hub for chemical and biological technical expertise. The JSTO, which leads the defense community in preparing for chemical and biological threats, identifies and provides cutting-edge technology solutions to protect the security of the American people while empowering warfighters to achieve their missions in dangerous environments. The JSTO is responsible not only for protecting against the known threats of today but also for anticipating the major threats of tomorrow. In addition, JSTO provides science and technology support to the Department of Defense, other government agencies, and the international community.

DTRA sponsored more than 300 U.S. government, academia, and industry representatives as participants for CBOA 22, which addressed military capability gaps and high-priority mission deficiencies. During the week-long event, new CBRN-related technologies were assessed by capturing user feedback from all branches of the U.S. armed forces. Technologies were rated at technology readiness levels ranging from three to eight, based on four mission areas corresponding to the CBRN core functions: assess, protect, mitigate, and integrate command and control management. The assessment focused on the following characteristics of the technologies: performance, adaptability, ability to be integrated into the mission command common operating picture, digital security, environmental robustness, training burden, ease of use, task-load requirements for system operations, propensity for system malfunctions, routine maintenance burden, and logistical impacts. The event consisted of three lanes, which contained multiple operational scenarios to demonstrate the effectiveness of the technologies.

CBRN Protection 2030 and Beyond

According to Army Doctrine Publication (ADP) 3-37, *Protection*, "Many state and nonstate actors (including terrorists and criminals) possess or have the capability to possess, develop, or proliferate [weapons of mass destruction] WMD. The most likely adversaries during large-scale ground combat have significant WMD capabilities and the doctrine to employ them during conventional operations. The training to conduct operations in a WMD environment is critical to operational success."[1] In order to achieve freedom of action, increase lethality, and enable movement and maneuver in the execution of large-scale ground combat operations in the complex CBRN environment, the Army must aggressively develop future CBRN defense capabilities to outpace our adversaries.[2]

U.S. Army Futures Command (AFC) Pamphlet (Pam) 71-20-7, *Army Futures Command Concept for Protection 2028*, builds upon the ideas of the multi-domain operations concept and serves as the baseline for required CBRN protection capabilities to enable Army forces in multi-domain operations through CBRN reconnaissance and surveillance, integrated early warning, real-time understanding, inherent survivability, and mitigation of CBRN hazards.[3] The key to successful all-domain protection includes improvement of artificial intelligence and machine learning for CBRN detection and mitigation capabilities. CBOA 22 highlighted breakthrough scientific discoveries and technological innovations that support the central idea of the core CBRN competencies (assess, protect, and mitigate) and the integrating activity of hazard awareness and understanding in support of the *United States Army Chemical Biological Radiological Nuclear (CBRN) Science & Technology Strategy*.[4] By employing capabilities that enable decision making and protect the force, commanders can sense, assess, understand, decide, and act faster and more effectively, thereby gaining an information advantage.

CBOA Technologies Overview

CBRN assessment capabilities enable commanders to understand the environment as early as possible so that they may make informed, risk-based decisions that protect the force while retaining freedom of action in a CBRN environment. The following assessment technologies were assessed during CBOA 22:

- **Dial-a-Threat Assay**—a hand-held, unpowered, human-readable biological threat identifier.
- **Biological Automated Collector/Detector for Expeditionary Reconnaissance (BioACER©)**—a fully automated biological collection and identification device that can be released from an unmanned arial system (UAS) for remote analysis over a plume.

- **Falcon 4G©**—a 4th-generation laser-based CBRN standoff detector (which was used in a base defense scenario).
- **FentAlert©**—an all-environments screening assay for pharmaceutical fentanyl-based agents.
- **Far-Forward Advanced Sequencing Technology**—a technology used to identify DNA- or RNA-based organisms.
- **Hazardous-material small UAS**—a UAS that is used to fly optimized patterns through hazardous areas, detecting, identifying, quantifying, and mapping hazardous data in real time, thereby enhancing situational awareness and improving decision quality.
- **MUSA P3I©**—a semiautonomous quadrupedal robot with integrated chemical and radiological detection/identification instruments that can also take photographs in the hot zone and conduct most CBRN reconnaissance/sampling missions.
- **NuGBall©**—a portable sensor network for real-time CBRN contamination mapping.
- **Pendar X10©**—a handheld standoff Raman spectroscopy chemical identification system used to identify unknown materials (liquid, solid, gel) at a distance of 1 to 6 feet within a few seconds (Figure 1).

Figure 1. Pendar X10

- **Raman spectrometer**—a spectrometer used to identify collected particles.
- **Rigaku©**—a portable handheld, dual-technology 1064 nanometer for the identification of chemicals and toxic industrial chemicals.

CBRN protection capabilities enable inherent survivability (individual and collective) in support of large-scale combat operations, without degradation or loss of combat effectiveness in a CBRN environment. The following protection technology was assessed during CBOA 22:

- **Second Skin©**—a mask cover that is installed on a standard M50 mask to improve the protective garment hood and mask interface.

CBRN mitigation contributes to the negation of hazard effects by providing commanders the flexibility to make risk-based decisions about the mitigation of residual CBRN contamination without the reduction of combat power or unnecessary expenditure of time and resources. The following mitigation technology was assessed during CBOA 22:

- **Decontaminating skin soap**—a soap that is used to rapidly decontaminate sensitive equipment, materials, and skin from chemical warfare agents, biological warfare agents, toxic industrial chemicals, toxic industrial materials, nontraditional agents, pharmaceutical-based agents, and other emerging threats.

Digital Battlespace Command and Control Management

Digital battlespace command and control management systems provide CBRN staffs with the information required for commanders to make decisions with enhanced situational awareness and understanding in a timelier manner. Digital battlespace command and control management tools allow CBRN staffs to receive large amounts of CBRN threat information and intelligence, conduct analysis, and develop trends related to enemy CBRN employment. Technology developers presented the following capabilities during CBOA 22:

- **CBRN Analysis Software**—a commercial, off-the-shelf knowledge management application.
- **The Hazard Estimation and Assessment Toolkit**—a next-generation CBRN hazard modeling application for web-based TAK and Windows© TAK platforms.
- **Multiintelligence-Enabled Discovery**—artificial-intelligence, machine-learning algorithms that use Azure Cloud© and Azure Cognitive Services© to provide near-real-time processing of multiple types of raw, unformatted environmental and intelligence data to provide intelligence insight and information to decision makers.

Conclusion

CBOA forges the future of CBRN modernization by showcasing experimentation, demonstration, and capability development for the joint force. Commanders need the ability to see the adversary, deny it anonymity, counter specific strengths, achieve positions of advantage, and expand and exploit gained areas. Lieutenant General D. Scott McKean, director of the Futures and Concepts Center, Army Futures Command, Fort Eustis, Virginia, prefaced his CBOA 22 speech on AFC Pam 71-20-7 by stating, "Looking forward, the Army must develop capabilities that can support and integrate with our joint, interagency, interorganizational, and multinational partners to expand the protection capability, increase capacity in competition, and operate at scale in armed conflict." This guidance exemplifies the Army commitment to protecting the force, improving survivability, and reestablishing the readiness of forces through the development of modernized capabilities.

Endnotes:

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

[2]*CBRN Operations Force Modernization Strategy*, U.S. Army CBRN School, Fort Leonard Wood, Missouri, July 2018.

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

[4]*United States Army Chemical Biological Radiological Nuclear (CBRN) Science & Technology Strategy*, U.S. Army, 2022.

Chief Warrant Officer Three Brown is a material development technician assigned to the Combating Weapons of Mass Destruction Branch, Requirements Determination Division, Futures and Concepts Center, Maneuver Support—Capabilities Development and Integration Directorate, Army Futures Command, Fort Leonard Wood, Missouri. He holds an associate of arts degree from Central Texas College and a project management professional certificate from the Project Management Institute.

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	21 August 2019
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*	ALSA/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:

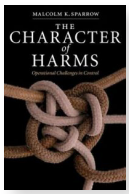
ADP—Army doctrine publication
ALSA—Army Air, Land, Sea Application
ATP—Army techniques publication
CAC—U.S. Army Combined Arms Center
CADD—Combined Arms Doctrine Directorate
CASCOM—U.S. Army Combined Arms Support Command
CCoE—U.S. Army Cyber Center of Excellence
EOD—explosive ordnance disposal
FCoE—U.S. Army Fires Center of Excellence
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

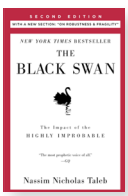
7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War, John F. Antal, Casemate, 2022. The Nagorno-Karabakh War was the first war in history to be won primarily by robotic systems, and its impact on the protection warfighting function cannot be overstated.



The Character of Harms: Operational Challenges in Control, Malcolm K. Sparrow, Cambridge University Press, 2008. 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.

Breaking Doctrine Podcast, Episode 7: "Protection," Major Chris Parker, Combined Arms Doctrine Directorate, Fort Leavenworth, Kansas, 2021. 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.

Critical Infrastructure Protection: Assessing the Risk in the Post Pandemic, Homeland Defense and Security Information Analysis Center, 15 September 2021, <http://hdiac.org/webinars/critical-infrastructure-protection-assessing-the-risk-in-the-post-pandemic/>, accessed on 22 August 2022. The Homeland Defense and Security Information Analysis Center, Belcamp, Maryland, offers many compelling and useful webinars and published articles; in this webinar, the agency examines how the Novel Coronavirus (COVID-19) pandemic has posed new challenges for critical-infrastructure protection. This session reviews traditional and emerging risks and discusses the steps needed to safely manage the overall change in the risk paradigm.

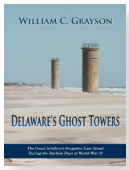


The Black Swan: The Impact of the Highly Improbable (2d edition), Nassim Nicholas Taleb, Random House, 2010. This update of the 2007 classic discusses risk, future planning, and the role of an almost infinite number of highly unlikely and unforeseen events—a "must-read" for the protection planner.

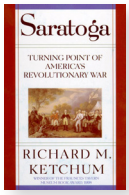
Modernization

Army Readiness and Modernization in 2022, Land Warfare Paper 146, Latashia Bates, the Association of the U.S. Army, Arlington, Virginia. This paper presents a perspective on what the Army is doing across its three priority efforts, providing context for the concepts of readiness, modernization, and people first.

History



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. 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. 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. 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, enlisted Soldiers, warrant officers, 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 not referenced in the text, appropriate endnotes should be provided. 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 in 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.

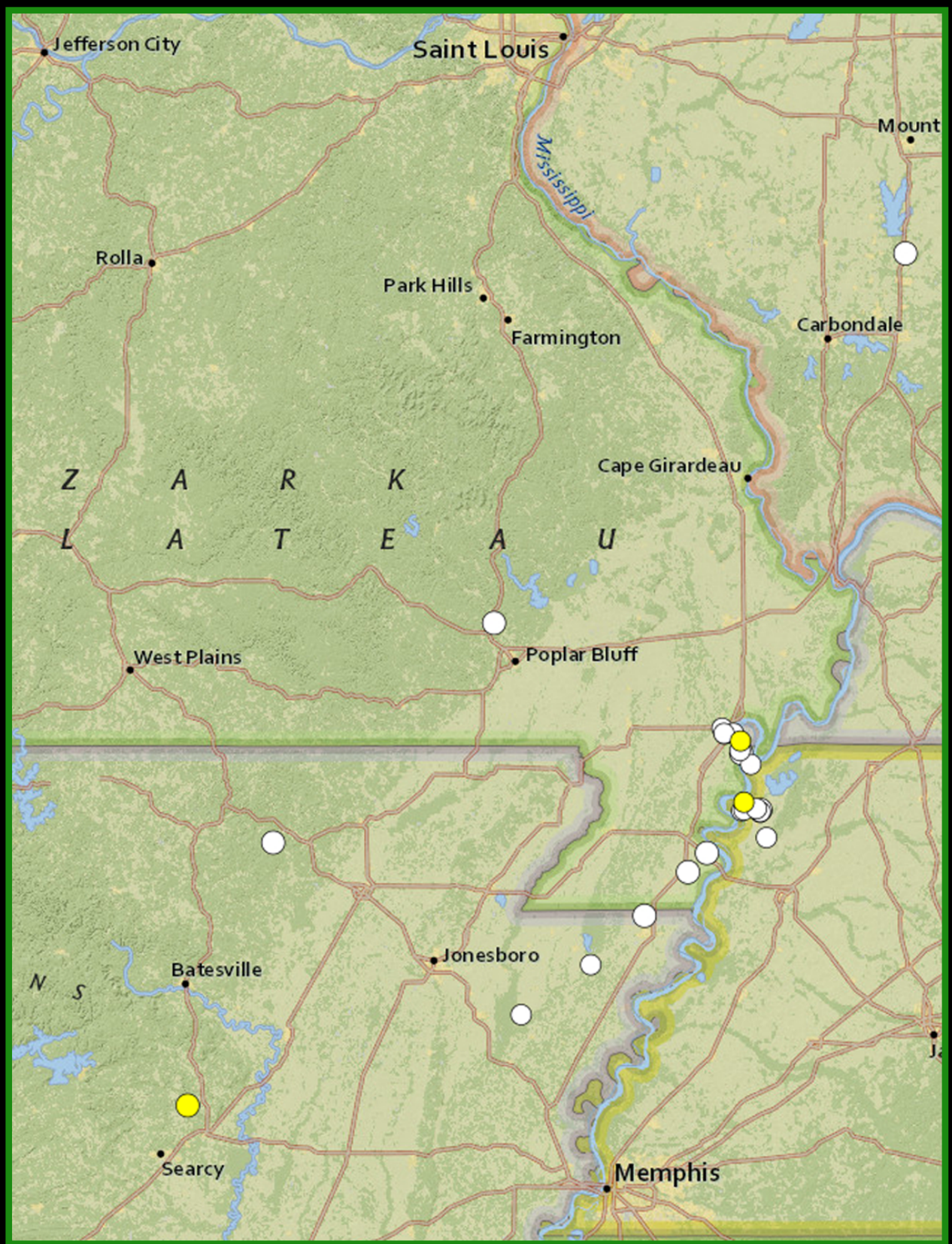
Provide a short paragraph that summarizes the content of the article. Also include a short biography, including your full name, rank, current unit, job title, and education; your mailing address; a fax number; and a commercial daytime telephone number.

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 print articles that have been accepted for publication at other Army venues.



This map shows the epicenters of several minor earthquakes that occurred in the New Madrid Seismic Zone (located between St. Louis, Missouri, and Memphis, Tennessee) during July 2022. Experts estimate the probability of an earthquake with a Richter magnitude of 6.0 or greater (a very high-impact event requiring a whole-of-government response) in this zone within the next 50 years to be 25–40 percent.

PIN:213111-000