POWER PROJECTION MISSION ASSURANCE IN THE HOMELAND

By Mr. Matthew K. McLaughlin

Since before the turn of the last century, the United States has realized the benefits of fighting its wars on the territories of other nations. With the exception of the raid on Pearl Harbor, geography has enabled the United States to prevent attacks with major military impact at relatively low cost. We have enjoyed a secure bastion from which to project national power in support of our national security and that of our allies. Even the 11 September 2001 attacks, although similar to the Pearl Harbor raid in that they targeted unaddressed vulnerabilities, caused no disabling damage to major military capabilities.

The United States can no longer count on the advantage of the homeland as a secure sanctuary from which to project power. An ever-more accessible world continually increases the vulnerability of domestic capabilities that support warfighting. Attempts by North Vietnamese and North Korean actors and their allies to leverage a free press and undermine American popular support for U.S. engagements in Southeast Asia are well-documented. Soviet leaders in the 1980s conducted extensive studies of American power projection capabilities and dependencies and developed plans to attack them with a range of options.[1] More recent documents, including the latest U.S. Army Training and Doctrine Command (TRADOC) operational environment publication, *The Operational Environment (2021–2030): Great Power Competition, Crisis, and Conflict,*[2] outline the likelihood of attacks on the United States to deter, degrade, disrupt, delay, or destroy U.S. forces before they can depart the homeland and highlight the need for improved intelligence, protection, and coordination capabilities to address the threats. Continually increasing access to, and dependence on, space, cyberspace, and global information and transportation networks promises to accelerate the growth of both threats and vulnerabilities into the foreseeable future. Due to these realities, it is imperative that Army professionals recognize protection in the homeland as a critical enabler of great power competition across the continuum of conflict.

TRADOC Pamphlet (Pam) 525-3-1, "The U.S. Army in Multi-Domain Operations 2028," referred to as the multi-domain operations concept,[3] describes a future operating environment that is substantially more complex and challenging than that of even the recent past. The concept outlines the need for the United States of the future to expand the competitive space, win in competition, deter escalation to armed conflict and, if necessary, win in armed conflict and return to competition on more favorable terms. This strategy depends heavily on the credible ability to synchronize the projection of military power from the homeland in all domains, the information environment, and the electromagnetic spectrum to decisive spaces across the multi-domain operations framework in response to aggression.[4]

The projection of military power from the homeland is key to the coordinated exercise of the diplomatic, informational, military, and economic instruments of national power to achieve national strategic goals. These elements of power, particularly the military element, are heavily dependent on public- and private-sector capabilities in the homeland. Military, public-sector, and private-sector capabilities comprise the power projection enterprise. This enterprise draws its effectiveness and resilience from the Service members, employees, and decision makers who make up the organizations. In short, it is the people of the United States who are the source of its strength, as it is the people of the United States whose interests are represented by U.S. strategic goals. This relationship is illustrated in Figure 1.

Adversaries challenge our multidomain power projection strategy by effective execution of antiaccess strategies against the homeland to create and maintain layered stand-off, denying friendly multidomain access from the homeland. They thereby intend to achieve strategic aims below the threshold of armed conflict before friendly power projection can be brought to bear. Unlike in forward areas, however, much of this activity is directed against the people who enable power projection, many of whom have no direct connection with the military. Adversaries conduct cyberspace and information activities to reduce resilience by attacking societal cohesion and confidence in the government during competition, escalating activities to more damaging measures as they progress along the competition continuum. Intelligence collection, the development of sympathetic populations into clandestine actors, and the resourcing of criminal elements provide means for adversaries to stymie friendly power projection.

None of this is new. Adversaries have always attempted to compromise home front support. Similarly, there has always been a need to protect the homeland power base from these actions. The difference with the emerging and future operating environment is the extent to which modern technology enables adversarial efforts. The interconnectedness of infrastructure and society enhances the potential reach and impact of adversarial efforts. Ready access to, and the rapid diffusion of, information via the Internet/social media amplify and accelerate interactions between people, governments, militaries, and threats, as observed with the Russo-Georgian war of 2008, the Arab Spring of 2010–2012, and the ongoing Russo-Ukrainian conflict. Artificial intelligence and deep fake technologies allow adversaries to dynamically distort perceptions of target populations while optimizing well-disguised cyberattacks against critical power projection targets. This emerging ability to execute optimized and coordinated attacks across the many military, public, and private components of the power projection enterprise requires

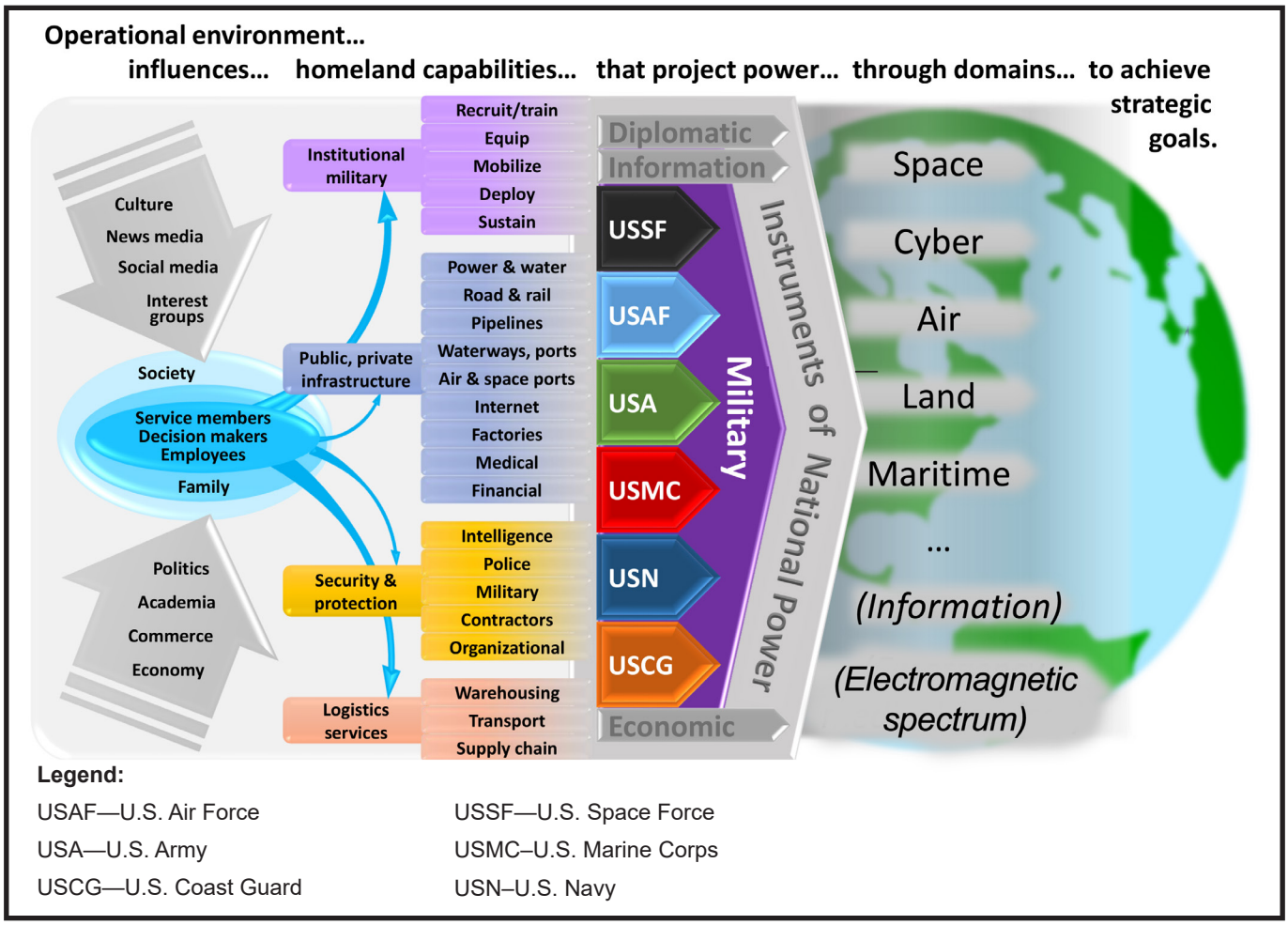


Figure 1. The power projection enterprise

a new approach to protection in the homeland. Power projection mission assurance must be a key factor in the development of future plans and capabilities.

U.S. Army Futures Command Pam 71-20-7, *Army Futures Command Concept for Protection 2028,* describes how the force will execute protection in the future operating environment.[5] The concept identifies three central components of the solution for the Army protection warfighting function:

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

This list recognizes that the operational Army requires more than the traditional solution of passive protection measures—the future force must proactively deny and defend against enemy action. This proactive approach comes naturally to warfighters in forward areas, where action and initiative are key to survival and success. The Army protection warfighting function is a robust toolbox that commanders can use to preserve and ensure the availability of operational capabilities in this environment.

However, the Army protection warfighting function doesn't address the operational and resiliency requirements of the domestic power projection enterprise, particularly in the public and private sectors—nor do other protection programs and capabilities. Army Regulation (AR) 525-2, *The Army Protection Program*, addresses the protection requirements of homeland installations, but it neither prioritizes support to combatant commanders nor addresses public- and private- sector enablers.[6] Homeland defense, homeland security, and defense support of civil authorities programs address the protection needs of the homeland as a whole, but without specific consideration for power projection requirements. Joint Publication (JP) 3-0, *Joint Operations,* discusses domestic installations and related capabilities under the joint protection function, but only in general terms.[7] Our allies also contribute protection capabilities; but again, without a focus on U.S. power projection. Figure 2, page 28, illustrates the various needs and solutions/programs for the protection mission space.[8]

While the Army protection warfighting function addresses the needs of operational forces, the resiliency and responsiveness requirements of power projection form the basis of argument for the application of its components across the power projection enterprise. The application of these components in support of power projection mission assurance requires a deliberate approach. The Army must integrate these components into its power projection capabilities, and it must team with its power projection partners in the public and private sectors to support the development of these characteristics in their supporting capabilities.

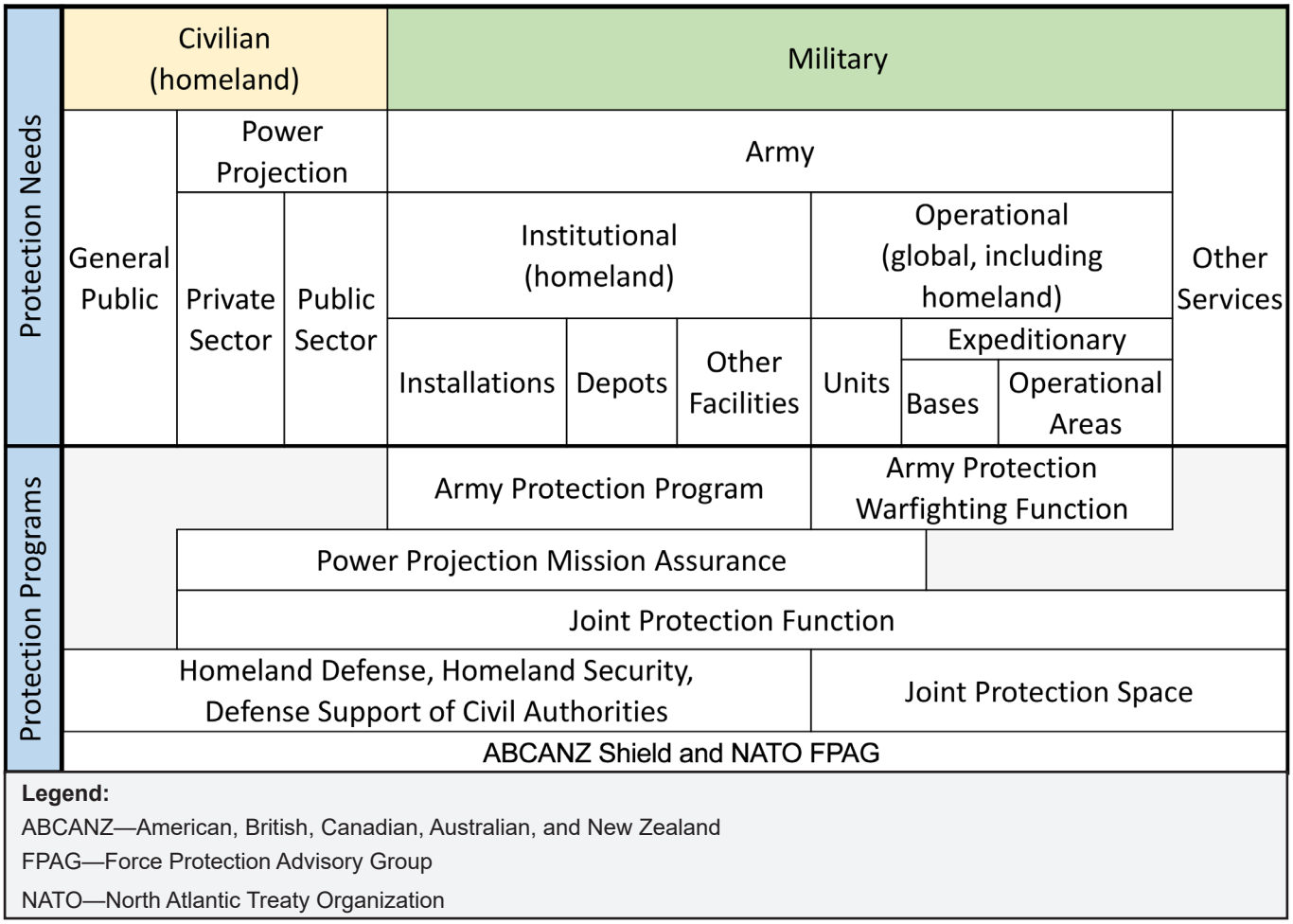


Figure 2. The protection mission space

The Army must be able to execute multidomain power projection against a near-peer threat by pushing ready-to-fight forces in concert with effects in multiple other domains. This must be accomplished from domestic facilities under various levels of multidomain attack. From a protection perspective, this requires the ability to deny the threat freedom of action against—and ensure preservation of—critical capabilities, assets, and activities across the power projection enterprise while enabling persistent access to all domains, the information environment, and the electromagnetic spectrum.

Installations must be "operationalized" to enable expeditionary maneuver from threatened installations, through contested lines of communication, to strategic distances in a matter of days, while protecting tenant organizations from enemy action. This requires the transformation of the installation enterprise culture from one with an administration- and management-based focus to one with an operational focus that makes it an integral partner in the warfight.

Power projection platforms require a significantly increased ability to preserve critical capabilities, assets, and activities, including tenant and transient units in the case of installations. They must also have built-in resilience and redundancy to enable persistent multidomain access in support of combatant commanders. They must provide protection against surveillance and reconnaissance as well as against attacks in all domains, the information environment, and the electromagnetic spectrum.

Installations, facilities, and infrastructure must be modernized and resourced to provide intelligent, robust, and secure power projection. These updates must emphasize the continuity of operation under conditions of attack or disaster and the ability to be rapidly restored to full operation following adverse events as well as the capacity for cost-effective incorporation of emerging advanced technologies.

The successful execution of multi-domain operations requires public- and private-sector enablers that possess mission assurance characteristics similar to those required by the Army. Similarly, the resilience of individuals and Families that is considered fundamental to expeditionary Soldiers is also required of enabler work forces, which are now subject to threat action. The Army must develop a deep and well-documented understanding of its dependencies on external partners, their limitations in supporting these dependencies, and the threats to which they may be subjected. The Army must then communicate these requirements to its partners in a straightforward and convincing manner and cooperate with them in developing security solutions and protection measures while supporting updates to contracting requirements and interagency policy. In many cases, the Army must develop ways to encourage and incentivize these enablers to invest in these capabilities, which are not inherently profitable to their daily activities.

Power projection mission assurance requires the full integration of the key ideas of the Army protection concept across the entire power projection enterprise. The Army

and its partners must preserve strategic projection capacity against robust oppositional action in the homeland and deny enemy freedom of action through the development and operation of multidomain resilient capabilities. This is fundamental to persistent access for multidomain strategic maneuver in support of mission commanders. Army power projection mission assurance will continue to heavily depend on the Army Protection Program and joint force protection capabilities, which must evolve to support the operationalization of the installation enterprise. The synchronization of these aspects of protection and the extension of the military protection mindset to the Army's public- and private-sector partners are critical to power projection. Army leaders must integrate these homeland considerations into their strategic calculus to provide the firm foundation required for victory in emerging and future operating environments.

Endnotes:

[1]Graham H. Turbiville Jr., "Prototypes for Targeting America: A Soviet Assessment," *Military Review*, January–February 2002.

[2]"The Operational Environment (2021–2030): Great Power Competition, Crisis, and Conflict," TRADOC, <https://oe.tradoc.army.mil/2021/10/04/the-operational-environment-2021-2030-great-power-competition-crisis-and-conflict-2/>, accessed on 12 October 2021.

[3]TRADOC Pam 525-3-1, *"The U.S. Army in Multi-Domain Operations," 2028*, 6 December 2018.

[4]The multi-domain operations concept defines strategic space as a conceptual geographic and temporal location where the full optimization of the employment of cross-domain capabilities generates a marked advantage over an enemy and greatly influences the outcome of an operation. The need to converge capabilities at a particular place and time to create or leverage a window of superiority highlights the requirement for dependable multidomain power projection capabilities.

[5]U.S. Army Futures Command Pam 71-20-7, *Army Futures Command Concept for Protection 2028*, 7 April 2021, <afc-pam-71-20-7-afc-protection-concept-vfinal-apr21.pdf >, accessed on 4 October 2021.

[6]AR 525-2, *The Army Protection Program*, 8 December 2014.

[7]JP 3-0, *Joint Operations*, 22 October 2018.

[8]The American, British, Canadian, Australian, and New Zealand Armies' Program Capability Group Shield and the North Atlantic Treaty Organization Force Protection Advisory Group contribute protection capabilities both at home and abroad, as shown in Figure 2.

Mr. McLaughlin recently retired as the chief of the Force Modernization for Homeland Defense/Civil Support Office, U.S. Army Maneuver Support Center of Excellence, Fort Leonard Wood, Missouri, where he managed the integration of homeland requirements into Army capabilities development. He is a retired U.S. Navy Reserve commander. He holds a master's degree in nuclear engineering from Missouri University of Science and Technology at Rolla.

("Scaffolding the Future . . . ," continued from page 25)

navigate the course (as should be the case). But that doesn't mean that the training developers aren't busy behind the scenes; they absolutely are!

The Protection Training Development Branch, Protection Division (Force Modernization Proponent), FFID, is hard at work, developing the tasks that will ultimately underpin the PIC terminal period of instruction. The overall goal of the branch is to generate 20 new Army tasks; so far, 11 new tasks have been generated. Each task is uniquely designed to address those gaps associated with the original DOTMLPF-P analysis and assessment. And in case you're wondering, task development is a long and technical process, often consuming upward of 100 hours per task to complete.

Finally, from our perspective here in the Protection Division, we are proud of the things that we have accomplished so far and are excited as we look forward to the things that we know are to yet to come. Each day, we see evidence of an ever-changing and more complicated operational environment and world. It is that evidence that propels our forward momentum. Perhaps most striking is the realization that protection training development capabilities are not only a pragmatic function of the protection domain; they are in fact, critical.

Endnotes:

[1]"Leonidas," *History.com*, 2019, <https://www.history.com/topics/ancient-history/leonidas>, accessed on 2 September 2021.

[2]Gregory J. Dehler, "Fabian Strategy," <https://www.mountvernon.org/library/digitalhistory/digital-encyclopedia/article/fabian-strategy/>, accessed on 2 September 2021.

[3]Brian J. Murphy, "Patton's Ghost Army," 2018, <http://www.americainwwii.com/articles/pattons-ghost-army/>, accessed on 2 September 2021.

[4]Michael P. Mahoney, *Striking a Balance: Force Protection and Military Presence*, Beirut, October 1983.

[5]Tim W. Quillin, *Force Protection in Support of Stability Operations*, 1999.

[6]Sun Tzu, *The Art of War,* 1521.

[7]U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (Pam) 350-7-9, *Budgeting and Resourcing*, 12 October 2012.

[8]Pilot status is a term used to describe an Army course that is in a temporary status due to a change or adjustment.

First Sergeant Koren (Retired) is a protection development analyst and the chief of the Protection Training Development Branch, Protection Division (Force Modernization Proponent), FFID, MSCoE. He holds a bachelor's degree in history from Drury University, Springfield, Missouri, and a master's degree in homeland security from George Washington University, Washington, D.C., and he is currently a doctoral student at the University of Southern California, Los Angles.