Aircraft formation flies over USS *George Washington* during combined U.S. and South Korean maritime and air readiness exercise

U.S. Navy (Charles Oki)

Defense Planning Paradigms and the Global Commons

By MARK E. REDDEN and MICHAEL P. HUGHES

Over the last several years, examination of U.S. national security interests within the context of the global commons has emerged as a major policy issue in the defense community.[1] At the highest levels of the Department of Defense (DOD), there is now an awareness that the U.S. military will be confronted by a host of challenges "to stability throughout the global commons."[2] Furthermore, the Nation can "expect to be increasingly challenged in securing and maintaining access to the global commons and must also be prepared for operations in unfamiliar conditions and environments."[3] In response, the 2010 *Quadrennial Defense Review Report* has now assigned "assured access" to the commons as a top priority for U.S. military forces.[4]

Captain Mark E. Redden, USN, and Colonel Michael P. Hughes, USAF, are Senior Military Fellows in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University. This article is based on *Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?* Institute for National Strategic Studies Strategic Forum 259 (NDU Press, November 2010).

As defined by DOD, the global commons comprise the geographic and virtual realms of "space, international waters and airspace, and cyberspace."[5] They are a subset of the broader maritime, aerospace, and cyber domains, deriving their existence from the notion of areas that are accessible to all but owned by none. The commons are seen as the essential conduits of U.S. national power in a rapidly globalizing and increasingly interconnected world. The heritage of the commons' strategic importance can be traced back at least as far as Alfred Thayer Mahan, who highlighted the relationship between maritime power and the ability to maintain the sea lines of communications with economic expansion and the impact on overall national power.[6] Attainment of U.S. strategic, economic, informational, and military objectives is contingent upon assured access to, and freedom of action within, the commons. Accordingly, global commons access must remain at the forefront of U.S. national security imperatives.

Successful application of military power in and through the global commons in

U.S. Air Force (Jim Varhegyi)

Air Force Vice Chief of Staff testifies before House Armed Services Subcommittee on Readiness about Air Force cyber security measures

support of overarching U.S. national objectives is likewise dependent upon the ability of military forces to access and maneuver within and across the commons—to deliver power in and through the various geographies. While the required extent and duration of the U.S. military's access to and freedom of action in the commons will be determined by larger strategic factors, the fundamental ability to achieve them is becoming more problematic. New complexities in the global commons potentially lessen military effectiveness, diminishing the military's ability to support national interests. Arguably, the least recognized and least understood of these complexities is the notion of domain interrelationships: the idea that *intradomain* military operations are increasingly dependent on *interdomain* dependencies.[7] Barring a fundamental shift in U.S. strategic objectives, the military must retain the ability to operate throughout the global commons to achieve the requisite level of local control and superiority for mission success in support of national objectives. To accomplish this, the U.S. defense establishment must reassess the fundamental ideas and concepts regarding military power employment within the global commons in light of expanding domain interrelationships.

New Challenges

Responsibility for the maintenance of the global commons and guarantee of free access for both international trade and commerce and the projection of military power has for more than 60 years fallen to the U.S. military.[8] However, over the last two decades, a confluence of events and emerging issues has begun to impact the U.S. military's ability to gain access to the global commons, as well as its freedom of action within it. The continuing evolution of the commons presents the U.S. military with a host of new challenges and demands.

First among these challenges is the incorporation of new geographies into the commons. In addition to dealing with growing complexities in the more "mature" maritime and air components, the U.S. military is confronting the issue of integrating the newer domains, space and cyber, into its fundamental concepts of operation. The cyber domain arguably provides the most acute challenge; its complex and at times seemingly anarchic nature and the difficulty in detecting and attributing actions complicate military planning. Despite its breadth of use within both the civilian and defense sectors, the U.S. defense community's understanding of the full impact of cyberspace on military capabilities and operations is modest at best.

Compounding the issue of the expanded scope of the global commons is their increasingly congested and contested nature. Driven in large part by economic and technological advances, barriers to commons access have been significantly lowered, with an attendant rise in the number and types of actors able to exploit the commons. For example, space—the almost exclusive purview of the superpowers during the Cold War due to high financial and technical barriers—is now routinely accessed by several dozen companies and consortia from various states, as well as individual entrepreneurs and commercial entities. Similarly, the oft-quoted price of access to the cyber domain can be as low as the cost of a laptop computer.

The dynamics making the commons more contested are varied and complex. At the high end, a number of state actors are rapidly approaching the level of a peer or near-peer military competitor in specific geographic areas. Although unable to challenge U.S. military access to all of the commons on a global scale and for extended periods of time, robust investment in conventional and asymmetric antiaccess and area-denial capabilities is positioning some countries to be able to challenge U.S. military access and freedom of action in bounded regions and for set periods of time. This is a significant issue given U.S. global interests and the military resources and efforts required to guarantee security of those interests at long distances.

Exacerbating the challenges from traditional or rising peer and near-peer military competitors is the increasing influence exerted by nonstate actors in the global commons. State actors typically have substantial incentives to keep general access to the commons unrestricted. Nonstate actors can have drastically different motives. Driven by such factors as economics and political ideology, nonstate actors are more likely to deny, restrict, or disrupt commons access and usage in pursuit of their objectives. Even a modestly sized nonstate actor can exert a disproportionate effect within the commons. As evidenced in the cyber domain, at little cost in resources and effort, small groups (or even individuals) can disrupt and degrade Internet access and functionality for civilian, commercial, and government users, yielding effects that are of far greater value than the costs of producing them.

The precipitous decline in U.S. conventional air and naval platforms used to address these challenges aggravates the situation. The global commons are expansive in nature, with time, speed, and distance factors that at times can only be addressed through employment of large numbers of military assets. In the air and maritime domains, current U.S. aircraft and ship quantities are a fraction of the levels that existed at the conclusion of the Cold War. In 2009, U.S. Navy ship numbers alone were over 50 percent lower than they were in 1990 in the waning days of the Cold War.[9] While technological advances help offset the negative aspects of force reductions, they are insufficient to address the growing challenges inherent in a more complex and dynamic global commons. In the cyber domain, resource challenges are exacerbated by the complex balance between offense and defense and the difficulty of attempting to innovate in a military field while simultaneously responding to the advancements of others. Unlike the maritime, air, and space domains, where the United States has traditionally been at the forefront of military development and has compelled potential adversaries to respond to its military initiatives, the Nation has no such advantage in the cyber domain.

External and internal fiscal pressures will limit the near- to mid-term potential for significant growth in the defense procurement budget. Furthermore, the short-term requirement to balance current counterinsurgency and counterterrorism operations against other mission requirements makes the prospects for a resource-intensive solution to the challenges posed within the global commons unlikely. The U.S. military will not be able to apply overwhelming quantitative and qualitative resource advantages to solve global commons problems.

The last and least recognized military challenge in the global commons involves the rapidly developing interrelationships among and between the different domains and the platforms and systems operating in and through the related parts of the global commons. The phenomenon is a manifestation of how military capabilities and operations have evolved, particularly over the last two decades. Domain interrelationships start at the most fundamental levels of military operations and capabilities and yield effects throughout the whole spectrum of military power as the totality of the interrelationships is integrated across each level of warfare. Now more than ever, effective and efficient application of military power in any specific part of the global commons rests upon a foundation of simultaneous access and freedom of action throughout the remainder of the commons. The idea of domain interrelationships is not new. These interrelationships have been, to a certain degree, part of military planning for as long as the potential for multidomain military operations has existed. Rather, it is the breadth of the various domain interrelationships and the pace at which they have developed that are now the critical issues.

Domain interrelationships cover a wide spectrum of dependencies between platforms and systems and, ultimately, operations. At the low end of the interdependence scale are interrelationships that enhance capabilities and provide force multipliers. This degree of interrelationship does not preclude employment of military power in a particular domain, but helps increase the effectiveness of platforms and systems. At the other end of the spectrum stand true interdependencies: interrelationships that can preclude operations in one domain if access to other domains is denied. Defense leaders have provided illustrative discussion on these evolving interrelationships and the global commons, particularly with respect to the space and cyber domains. However, taxonomies matter a great deal when distinguishing relationships that are interconnected (and therefore enabling) from those that are mutually dependent (and therefore require access to other domains).

Despite the increasing importance of domain interrelationships, development of military strategy and fundamental concepts of operations for the employment of military power within the commons has not kept pace. The increasingly congested and contested nature of the commons and the problem of declining U.S. conventional force levels do not necessarily lend themselves to quick fixes and will continue to stress the military's ability to ensure continued access to the commons. To prevent any further reduction in the margins of its military superiority, the United States must seek to optimize its military capabilities in the global commons despite these constraints. The U.S. defense establishment must revisit the fundamental ideas and concepts regarding the employment of military power within the global commons in light of growing domain interrelationships.

The New Reality of Domain Interrelationships

Historical perspectives on military use of the global commons from the industrial age detail a long period of modest advances in capability and domain interactions. Military exploitation of each new geography, along with its integration with the others in the context of military operations, was modest in scope and relatively linear in nature, occurring over extended timeframes. Despite the work of General Billy Mitchell and others in the interwar period of the 1920s and 1930s, the full appreciation of airpower's utility in maritime operations arguably was not realized until World War II, some 30 years after the initial exploitation of the air domain for military purposes. The advent of the information age induced a marked shift in this dynamic. The technology that drove the information age significantly increased the range of militarily useful tools and resources, enhanced intradomain capabilities, and, more importantly, yielded a range of previously unavailable interdomain military options.

At the tactical level, advocates of platforms specific to each individual domain have continued their relentless pursuit of intradomain dominance, while exploiting technology-based capabilities that require access to other domains. As an example, the F–22 represents the premier air superiority aircraft, with its unequalled radar-evading technologies, engine performance, and advanced avionics; it also provides additional force multipliers such as unique connectivity and electronic attack capabilities. However, the latter capabilities are wholly dependent upon the ability of the aircraft to access the space and cyber domains. As the DOD aircraft investment plan for fiscal years 2011–2040 points out, "When considering aviation investment plans, the Department must increasingly consider the potential complementary capabilities resident in the cyber and space domains, as well as across other aircraft types."[10] The F–22 highlights how military operations within the global commons are now multidomain in nature, with interrelationships that can simultaneously span all domains and blur the distinction between supported and supporting efforts. Adding to this complexity is the growing overlap between the military and civilian realms, with military capabilities becoming increasingly reliant on commercial satellite communication systems, space-based surveillance, and cyber infrastructure for mission success.

With space and cyberspace serving as the bond between a range of military capabilities that require access to the commons, domain interrelationships have become more pervasive and complex. These interrelationships alter basic notions of force-on-force analysis. Drawing a parallel from cyber and telecommunications network theory, the intrinsic value of military platforms and systems can conceivably increase at a nonlinear rate with the linear addition of each new platform and system, in large part due to the multitude of interrelationships.[11] A logical and corollary lesson is that vulnerabilities may expand at a nonlinear rate as well, with the associated risk to U.S. military operations increasing rapidly. Further proof of the importance of domain interrelationships exists in capabilities derived from exploitation of the space domain. Loss of space systems, whether involving the global positioning system constellation, communications systems, or intelligence, surveillance, and reconnaissance assets, would have negative effects that would cascade across military platforms and systems in other domains. This example illustrates how a limited number of key tactical level interdomain relationships can yield operational level effects.

the growing reliance of military systems and operations on commercial enterprises is but one possible insidious relationship that puts U.S. military capabilities at risk and that is largely unseen without a macro view of the complex, interactive system that is the global commons

The manner in which space and cyberspace now provide a means for the transmission of military power distorts traditional industrial age notions of supporting and supported domains. The increasing capacity for space and cyber to become the primary focus of effort within a military operation can lead to role reversals. For example, with a significant portion of the cyber domain relying on seabed transmission cables, efforts to disrupt military operations in cyberspace could employ maritime and air domain operations as supporting elements. The multiorganizational Operation *Burnt Frost* in 2008, which led to the destruction of a malfunctioning U.S. reconnaissance satellite, provides a real-world example: maritime domain operations (primarily) were conducted in support of operations in space, traditionally considered an enabling or supporting domain.

The Traditional Approach

Throughout history, the emergence of human activity within each of the sea, air, space, and cyberspace domains has produced a fundamental transformation in the nature of warfare and military operations. It is this geographic aspect of warfare, albeit on a domain-by-domain basis, that has remained a cornerstone for the U.S. military approach to development of military power theory and operating concepts. This reductionist, bottom-up methodology arguably propagated a degree of stovepiping in strategy and concept development within the commons. Development tends to proceed in a linear and highly dogmatic fashion, with a focus on single domain exploitation preceding efforts to address the implications of domain overlaps and interdependencies. Much as was the case for air and maritime doctrine, development of concepts for military operations within the space domain (and more recently in cyberspace) appears to be following a similar pattern, with intradomain analysis and concept development preceding interdomain considerations. The U.S. Air Force and Navy have only just begun efforts to better understand the implications of cyber warfare for air and maritime operations; these nascent efforts are perhaps less well developed than the modest understanding of military operations exclusive to the cyber domain itself.[12] Bi-domain theoretical initiatives have typically been marked by a hierarchical conceptual approach in which one domain is dominant and the other exists in a subordinate or supporting role. While the military operating environment in and through the commons shows ever-increasing degrees of complexity, the theoretical methodologies used to address this environment have not kept pace.

Why a New Approach?

The traditional approach to conceptual development that begins with intradomain work followed by measured bi-domain expansion lags the transformational nature of current opportunities and challenges in the global commons. The implications of these growing challenges are not insignificant. The growth of cross-domain interrelationships brings a concomitant increase in the number of seams between the domains—seams that offer large numbers of both vulnerabilities and opportunities. Approaching conceptual development for the commons with a stovepiped, single domain–centric mindset heightens the risk that domain dependencies and the resulting seams will be inadequately addressed. Given integrated and highly interdependent domain relationships, degrading one system in one domain has the potential to exponentially increase degradation in all other systems. Serious analytical attention has not been devoted to cross-domain issues such as these, partly because a traditional stovepiped planning methodology is insufficient to identify and analyze the full scope and relevance of these issues.

Shortcomings in applying the traditional planning methodology to the global commons are not limited to the military realm. The growing reliance of military systems and operations on commercial enterprises (such as satellite communications and imagery) is but one possible insidious relationship that puts U.S. military capabilities at risk and that is largely unseen without a macro view of the complex, interactive system that is the global commons. The importance of operating from the global commons, and the increasingly complex relationships of platforms operating within the various domains, clearly requires a theoretical construct that accounts for these factors.

There appears to be a growing recognition within the U.S. military that the evolving nature of the global commons and the rapidly expanding set of domain interrelationships mean that traditional approaches to strategy and concept development may be ineffective. As pointed out by General Michael Moseley, former Chief of Staff of the U.S. Air Force, "Since the air, space and cyber domains are increasingly interdependent, loss of dominance in any one could lead to loss of control in all. . . . No future war will be won without air, space and cyberspace superiority."[13] The very fact that DOD has now unified the disparate geographies into the more encompassing term *global commons* and is pursuing a new multidomain theoretical initiative called AirSea Battle hint at the prospect that the notion of the global commons may be more than just a new, more convenient taxonomy scheme and may in fact be an initial attempt to recraft the strategy and concept development process. The critical issue for security planners thus becomes finding an appropriate methodology for development of a military

U.S. Navy (Joshua J. Wahl)

Navy Cyber Defense Operations Command Sailors monitor Navy information systems and computer networks for unauthorized activity

concept of operations for the global commons that goes beyond the domain-by-domain approach and fully considers the rich interactions between domains that characterize military operations in the commons.

Requirements of a New Planning Paradigm

Strategic thought has historically demanded consideration of a problem or issue in totality in order to grasp the full magnitude of the situation at hand. Whether for grand strategy development or military operational planning, a holistic perspective is required. Historically speaking, conceptual strategy development has always warned of the need for consideration of the whole in order to comprehend the overall nature of a particular military endeavor.[14] The same holds true for military planning when considering the need for operations conducted in any of the domains.[15]

Joint operating concepts in use today are designed to "identify future military problems and propose solutions for innovative ways to conduct operations. They are an articulation of potential future operations and describe how a commander, using military art and science, might employ capabilities necessary to meet future challenges."[16] Yet development of such concepts requires analysis that is not restricted to limited avenues of consideration (such as the air and sea domains as in the case of AirSea Battle). An analysis that envisions one or possibly two domains and considers others as enablers ignores the need to consider the totality of the global commons and the domains' evolving interdependent nature. As such, we should consider the global commons from a broader perspective.

While the body of intradomain research and concept development continues to evolve, parallel efforts that give full consideration to interdomain issues must also be conducted. An updated planning paradigm must fully quantify domain interrelationships, properly articulate the nature of the supported/supporting relationship for multidomain evolutions, seek synergies and leverage in military operations through the exploitation of domain overlaps, and ensure combat effectiveness by mitigating risks associated with seam vulnerabilities.[17] Strategists and defense planners must depart from the domain-centric mindset and take a broader perspective when viewing the commons. They must employ a holistic approach that breaks down domain stovepipes and treats the global commons not as a set of distinct geographies, but rather as a complex, interactive system.[18] It must not be merely an exercise in enhancing "jointness" within the force, but rather must be an issue of formulating a conceptual framework that allows us to think about, and plan for, military operations in this dynamic arena.

A paradigm shift to a macro perspective on a complex, interactive system that would provide the proper framework from which to address security and stability within the commons is needed to consider the global commons writ large. A Global Commons Operational Concept construct properly detailing the effective employment of military power to ensure commons access would serve not only military interests, but also broader national priorities within the diplomatic, economic, and informational realms as well. While at first appearing anathema to current doctrinal thinking, the intellectual exercise provides many benefits:

- it elevates thinking beyond the specific domains and forces a broader perspective that better accounts for the current reality of multidomain operations in the commons
- it forces consideration of the applicability of military missions (such as presence and power projection) into the newer domains of space and cyber
- it provides a framework to identify interrelated military-civilian-commercial connections that can affect military success.

The Way Forward

The United States must decide whether an increasingly congested, contested, and competitive global commons allows for a military strategy as straightforward as one that exploits a command of the commons. The answer is not self-evident. There is a clear need for a more detailed analysis of the global commons, along with a systematic determination of domain interdependencies, identifying the resultant risks and rewards and the appropriate means of incorporating them into military strategy, concepts, and doctrine.

Given current and evolving globalization and technological trends, we need a holistic paradigm to advance our understanding of military operations in and employing the global commons. This new perspective should better frame the nature of domain interdependencies and their potential impact on military power employment options. At a minimum, a holistic concept development methodology should quantify the nature of domain interdependencies, identify military vulnerabilities and opportunities associated with the domain seams, and illuminate fundamental principles of military power employment that will mitigate the risks associated with seam vulnerabilities and exploit inherent seam opportunities.

This interdependent nature is becoming clearer and much more pronounced. Yet the ability to operate freely in a secure and stable global commons is largely being analyzed using domain-specific constructs. Overarching questions must also be considered. What further research must be conducted to explore the interdependent relationships and maturing integration of the global commons? How do we define and comprehend the truly interdependent relationships that provide critical capabilities in a globalized world? Which dependencies are crucial to success when operating in the commons, and which linkages are merely enabling support? Have a common lexicon and taxonomy been clearly defined in order to consider the critical nature of the systems?

Multidomain interdependencies result in more complex challenges for military planners with regard to time, space (geography), and force issues given a particular objective or purpose. Joint operational planning emphasizes the importance of time and space and the need to comprehend these characteristics in and across particular domains. There is an increasingly critical need to more fully understand and exploit these cross-domain interdependencies, especially with respect to time disparities between the cyber domain and the other traditional domains. For example, the nearly instantaneous speed of movement in the cyber domain is very different from the time and space considerations that govern force employment in other domains. The implications for force planners used to focusing on maritime or air domains lie in the potential to exploit the speed of the cyber domain and ability to employ cyber assets at great geographic distances to increase the tempo of operations faster than ships can sail or aircraft can fly. However, this also implies that naval and air assets are now vulnerable to cyber attack from locations far removed from the battlespace. Air, space, or maritime forces reaching across their domains to influence or affect a force in another domain or multiple domains must now consider cyberspace's unique characteristics of speed, rapid pace of change, and influence on multiple domains in addition to the more traditional domains and their interrelationships.

From a military perspective, further consideration of a holistic global commons paradigm would inform strategy issues in a broader sense. What further analysis must be undertaken that informs or affects other aspects of military strategy, such as deterrence theory? Consideration should also be given to exploring the development of a military power theory for the global commons writ large. In addition, there should be analysis of an integration of a global commons military strategy into a global commons security strategy, and the resultant integration with other elements of national power and grand strategy, to ensure a synergistic approach to global commons research.

A paradigm shift must occur in order to fully comprehend the emerging systems nature of the global commons, and a military strategy and concept of operations are needed that fully consider the increasingly interrelated character of the various domains. Rapid technological advancements and improvements in military capabilities will continue to increase domain interdependencies within and across the global commons. As the United States and international community become more reliant on the global commons, a clear understanding of how to conduct multidomain military operations is needed if the United States is to have an effective strategy for maintaining military and commercial access to the global commons. **JFQ**

NOTES

[1] Michèle A. Flournoy and Shawn Brimley, "The Contested Commons," U.S. Naval Institute *Proceedings* 135/7/1,277 (July 2009), 1.

[2] Department of Defense (DOD), *Quadrennial Defense Review Report* (Washington, DC: DOD, February 2010), 8.

[3] Ibid., 103.

[4] Ibid.

[5] *National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, 2008), 13.

[6] Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660–1783* (New York: Dover Publications, 1987), 25.

[7] Throughout this article, no distinction is made between the broader notion of domain interrelationships and, as a subset of that, commons interrelationships. The important conceptual point is based upon the fact that military operation interrelationships across the geographies of space, air, maritime, and cyber are growing in scope and complexity. Utilization of the full physical extent of space, air, maritime, and cyber as opposed to the more bounded areas encapsulated in the notion of the global commons has little bearing on the central tenets of this paper. The terms *domain interrelationships* and *commons interrelationships* may be used interchangeably.

[8] *National Defense Strategy*, 16.

[9] "U.S. Navy Active Ship Force Levels," Naval Historical Center Web page, available at <www.history.navy.mil/branches/org9-4htm#1993>.

[10] Aircraft Investment Plan Fiscal Years (FY) 2011–2040, submitted with the FY 2011 Budget, February 2010, 3.

[11] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, DC: NDU Press and Potomac Books, Inc., 2009), 149.

[12] Chief of Naval Operations Strategic Studies Group XXVII, "Collaborate & Compel: Maritime Force Operations in the Interconnected Age," December 2008.

[13] General T. Michael Moseley, USAF, "The Nation's Guardians: America's 21st Century Air Force," Chief of Staff of the Air Force White Paper, Washington, DC, December 29, 2007, 2.

[14] Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 23.

[15] Joint Publication (JP) 5–0, *Joint Operation Planning* (Washington, DC: The Joint Staff, December 26, 2006), III–17.

[16] Deterrence Operations Joint Operating Concept, Version 2.0, December 2006, 1.

[17] At the operational level of war, the concepts of leverage and synergy are defined and placed as critical concepts in warfighting capabilities. In accordance with JP 5–0, *leverage* seeks, "in the context of joint operation planning, a relative advantage in combat power and/or other circumstances against the adversary across one or more domains (air, land, sea, and space) and/or the information environment sufficient to exploit that advantage." *Synergy*, "achieved by integrating and synchronizing the actions of conventional and unconventional forces and capabilities in joint operations and in multiple domains[,] enables Joint Force Commanders . . . to maximize available capabilities and minimize potential seams or vulnerabilities."

[18] "Simply defined, a *system* is a complex whole, the functioning of which depends on its parts- and the interaction between those parts. Simple systems can be characterized as having a few subsystems that are involved in only a small number of highly structured interactions. They tend not to change much over time, being relatively unaffected by the independent actions of their parts or by environmental influences. Extremely complex systems, at the other end of the spectrum, can be characterized as having a large number of subsystems that are involved in many more loosely structured interactions, the outcome of which is not predetermined. Such systems adapt and evolve over time as they are affected by their own purposeful parts and by the turbulent environments in which they exist." See Michael C. Jackson, *Systems Thinking: Creative Holism for Managers* (New York: Wiley, 2003), 3, 19.