Airpower, Spacepower, and Cyberpower

By BENJAMIN S. LAMBETH

Image of Baghdad showing smoke plumes from previous night's bombardment, acquired by IKONOS–2 satellite April 2003

NASA

When American airpower played a central role in driving Iraq's occupying forces from Kuwait in early 1991, many doubters tended to dismiss that remarkable performance as a one-of-a-kind force employment anomaly. It was, the doubters said, the clear and open desert environment, or the unusual vulnerability of Iraq's concentrated armored formations to precision air attacks, or any number of other unique geographic and operational circumstances that somehow made the Persian Gulf War an exception to the general rule that it takes "boots on the ground" in large numbers, and ultimately in head-to-head combat, to defeat well-endowed enemy forces in high-intensity warfare.

To many, that line of argument had a reasonable ring of plausibility when airpower's almost singular contribution to the defeat of Saddam Hussein's forces was an unprecedented historical achievement. During the 12 years that ensued in the wake of Operation *Desert Storm*, however, the world again saw American airpower prevail in broadly comparable fashion in four dissimilar subsequent cases, starting with the North Atlantic Treaty Organization's two air-centric contests over the Balkans in Operations *Deliberate Force* in 1995 and *Allied Force* in 1999, and followed soon thereafter by Operation *Enduring Freedom* against terrorist elements in Afghanistan in 2001–2002 and by the 3-week period of major combat in Operation *Iraqi Freedom* that ended Saddam's rule in 2003. Granted, in none of those five instances did the air weapon produce the ultimate outcome all by itself. However, one can argue that in each case, successful aerial combat and support operations were the pivotal enablers of all else that followed in producing the sought-after results at a relatively low cost in friendly and noncombatant enemy lives lost.

In light of those collective achievements, what was demonstrated by American air assets between 1991 and 2003 was arguably *not* a succession of anomalies, but rather the bow wave of a fundamentally new American approach to force employment in which the air weapon consistently turned in a radically improved level of performance compared to what it had previously delivered to joint force commanders. Indeed, that newly emergent pattern has now become so pronounced and persistent as to suggest that American airpower has finally reached the brink of maturity and become the tool of first resort by combatant commanders, at least with respect to defeating large enemy force concentrations in high-intensity warfare.

Yet in each of the five instances noted above, what figured so importantly in determining the course and outcome of events was not *airpower* narrowly defined, but rather operations conducted in, through, and from the Earth's atmosphere, backstopped and enabled, in some cases decisively, by the Nation's diverse additional assets in space and by operations conducted within cyberspace (that is, the electromagnetic spectrum).

Accordingly, any effort to understand the evolving essence of American *airpower* must take into account not only our aerial warfare assets, but also those vitally important space and cyberspace adjuncts that, taken together, have made possible the new American way of war. By the same token, any successful effort to build a theoretical framework for better charting the future direction and use of American air, space, and cyberspace

Benjamin S. Lambeth is a Senior Research Associate at the RAND Corporation. This article is an excerpt from his chapter in the forthcoming NDU Press book *Toward a Theory of Space Power: Selected Essays*, which is the outcome of the Institute for National Strategic Studies Spacepower Theory Project.

warfare capability must first take due measure of the Nation's current state of advancement in each domain. Toward that end, the discussion that follows offers a brief overview of where the United States stands today in each of the three operating mediums. It then considers some pertinent lessons from the airpower experience that bear on the development of spacepower and cyberpower theory, along with the sorts of cross-domain synergies that should be pursued in the many areas where the air, space, and cyberspace arenas overlap. Finally, it considers some essential steps that need to be taken toward that end before a holistic theory of warfare in all three domains, let alone any separate and distinct theory of spacepower, can realistically be developed.

Recent Air Achievements

By any measure, the role of airpower in shaping the course and outcome of the 1991 Persian Gulf War reflected a major breakthrough in the effectiveness of the Nation's air arm after a promising start in World War II and more than 3 years of misuse in the *Rolling Thunder* bombing campaign against North Vietnam from 1965 to 1968. At bottom, the *Desert Storm* experience confirmed that since Vietnam, American airpower had undergone a nonlinear growth in its ability to contribute to the outcome of joint campaigns at the operational and strategic levels thanks to a convergence of low observability to enemy sensors in the F–117 stealth attack aircraft, the ability to attack fixed targets consistently with high accuracy from relatively safe standoff distances using precision-guided munitions, and the expanded battlespace awareness that had been made possible by recent developments in command, control, communications, and computers, and intelligence, surveillance, and reconnaissance (ISR).[1]

As a result of those developments, American airpower had finally acquired the capabilities needed to fulfill the longstanding promise of its pioneers of being able to set the conditions for winning in joint warfare—yet *not* through the classic imposition of brute force, as had been the case throughout most of airpower's history, but rather through the *functional* effects now achievable by targeting an enemy's vulnerabilities and taking away his capacity for organized action. The combination of real-time surveillance and precision target–attack capability that was exercised to such telling effect by airpower against Iraq's fielded ground forces in particular heralded a new relationship between air- and surface-delivered firepower, in which friendly ground forces did the fixing and friendly airpower, now the predominant maneuver element, did the killing of enemy troops rather than the other way around.

During the years immediately after the 1991 Gulf War, further qualitative improvements rendered the Nation's air weapon even more capable. For one thing, almost every American combat aircraft now possessed the ability to deliver precision-guided weapons. For another, the advent of stealth, as was first demonstrated on a significant scale by the F–117 during the Gulf War, was further advanced by the subsequent deployment of the Air Force's second-generation B–2 stealth bomber that entered operational service in 1993. Finally, the advent of the satellite-aided GBU–31 Joint Direct Attack Munition (JDAM) gave joint force commanders the ability to conduct accurate target attacks with near impunity, around the clock and in any weather, against an opponent's core concentrations of power, whether deployed forces or infrastructure assets.

In the three subsequent major wars that saw American combat involvement (Operations *Allied Force*, *Enduring Freedom*, and the major combat phase of *Iraqi Freedom*), the dominant features of allied air operations were persistence of pressure on the enemy and rapidity of execution, thanks to the improved data fusion that had been enabled by linking the inputs of various air- and space-based sensor platforms around the clock. Greater communications connectivity and substantially increased available bandwidth enabled constant surveillance of enemy activity and contributed significantly to shortening the sensor-to-shooter data cycle time. Throughout each campaign, persistent ISR and growing use of precision munitions gave the United States the ability to deny the enemy a sanctuary. More important, they reflected an ongoing paradigm shift in American combat style that promised at the time to be of greater moment than was the introduction of the tank at the beginning of the 20th century.[2]

Since then, to be sure, mastering the sorts of lower intensity counterinsurgency challenges that have dominated more recent headlines has highlighted modern airpower's limitations as well as strengths. Although today's instruments of air warfare have thoroughly transformed the Nation's ability to excel in conventional warfare, those instruments and their associated concepts of operations have yet to have shown comparable potential in irregular warfare, since irregular opponents, given their composition and tactics, are less vulnerable than conventional opponents to airpower as currently configured and employed. Conversely, however, the recent rise of irregular warfare as our preeminent security concern today has been substantially a result of airpower's proven effectiveness in conventional warfare, a fact that attests to modern airpower's unprecedented leverage at the same time that it illuminates the continuing challenges that airpower faces.

friendly ground forces did the fixing and friendly airpower, now the predominant maneuver element, did the killing of enemy troops rather than the other way around

Space Contributions

The medium of space and its associated mission areas have also figured prominently in the steady maturation of American airpower since Vietnam. If there is a single fundamental and distinctive advantage that mature airpower has conferred upon theater commanders in recent years, it has been an increasingly pronounced degree of freedom *from* attack and freedom *to* attack for all force elements, both in the air and on the ground, in major combat operations. The contributions of the Nation's space systems with respect to both ISR and precision attack have played a central role in making those two force-employment virtues possible. Although still in its adolescence compared to our more developed air warfare posture, the Nation's ever-improving space capability has nonetheless become the enabler that has made possible the new strategy of precision engagement.

Despite that and other contributions from the multitude of military assets now on orbit, however, the Nation's air warfare repertoire still has a way to go before its post-Vietnam maturation can be considered

U.S. Army (Aaron D. Allmon II)

Airborne weapons officers monitor consoles aboard E–8C JSTARS aircraft

complete. Advances in space-based capabilities on the ISR front lie at the heart of the full and final transformation of American airpower. It is now almost a cliche to say that airpower can kill essentially anything it can see, identify, and engage. To note one of the few persistent and unrectified shortfalls in airpower's leverage, however, it can kill *only* what it can see, identify, and engage. Airpower and actionable real-time target intelligence are thus opposite sides of the same coin. If the latter is unavailing in circumstances in which having it is essential for mission success, the former will likely be unavailing also. For that reason, accurate, timely, and comprehensive information about an enemy and his military assets is not only a crucial enabler for airpower to produce pivotal results in joint warfare, but it is also an indispensable precondition for ensuring such results. In this regard, it will be in substantial measure through near-term improvements in space-based capabilities that the Air Force's long-sought ability to find, fix, track, target, engage, and assess any target of interest on the face of the Earth will become an established reality rather than merely a catchy vision statement with great promise.[3]

The spectrum of military space missions starts with *space support*, which essentially entails the launching of satellites and the day-to-day management of on-orbit assets that underpin all military space operations. It next includes *force enhancement*, a broader category of operations involving all space-based activities aimed at increasing the effectiveness of terrestrial military operations. This second mission area embraces the range of space-related enabling services that the Nation's various on-orbit assets now provide to U.S. joint force commanders worldwide. Activities in this second area include missile attack warning and characterization, navigation, weather forecasting, communication, ISR, and around-the-clock Global Positioning System (GPS) operations. A particularly notable aspect of space force enhancement in recent years has been the growing use of space-based systems for directly enabling, rather than merely enhancing, terrestrial military operations, as attested by the increasing reliance by all four Services on GPS signals for accurate, all-weather delivery of satellite-aided JDAMs.

To date, the American defense establishment has largely limited its space operations to these two rather basic and purely enabling mission areas. Once the third mission area, *space control*, develops into a routine operational practice, it will involve the direct imposition of kinetic and nonkinetic effects both within and through space. Conceptually, space control is analogous to the familiar notions of sea and air control, both of which likewise involve ensuring friendly access and denying enemy access to those mediums. Viewed purely from a tactical and technical perspective, there is no difference in principle between defensive and offensive space control operations and similar operations conducted in any other medium of warfare. It is simply a matter of desirability, technical feasibility, and cost-effectiveness for the payoff being sought.

Unlike the related cases of sea and air control, however, serious investment in space control has been slow to take place in the United States, in part due to a persistent lack of governmental and public consensus as to whether actual combat, as opposed to merely passive surveillance and other terrestrial enabling functions, should be allowed to migrate into space and thus violate its presumed status as a weapons-free sanctuary. The delay also has had to do with the fact that the United States has not, at least until recently, faced direct threats to its on-orbit assets that have needed to be met by determined investment in active space control measures, all the more so in light of more immediate and pressing research and development and systems procurement priorities. For both reasons, the space control mission area remains almost completely undeveloped. About all the United States can do today to deny enemy access to the data stream from space is through electronic jamming or by physically destroying satellite uplinks and downlinks on the ground.

Finally, the *force application* mission, which thus far remains completely undeveloped due to both widespread international disapprobation and a general absence of political and popular domestic support, will eventually entail the direct defensive and offensive imposition of kinetic and non kinetic measures from space in pursuit of joint terrestrial combat objectives. In its ultimate hardware manifestations, it could include the development, deployment, and use of space-

based nonnuclear, hyperkinetic weapons against such terrestrial aim points as fixed high-value targets (hardened bunkers, munitions storage depots, underground command posts, and other heavily defended objectives), as well as against surface naval vessels, armored vehicles, and such other targets of interest as enemy leadership. How many years or decades into the future it may be before such capabilities are developed and fielded by the United States has been a topic of debate among military space professionals for many years. For the time being, it seems safe to conclude that any such developments will be heavily threat-determined and will not occur, if only from a cost-effectiveness viewpoint, as long as effective air-breathing or other terrestrial alternatives for performing the same missions are available.

Fortunately, as the Nation's defense community looks toward further developing these mission areas in an orderly sequence, it can claim the benefit of a substantial foundation on which to build. In February 2000, the Defense Science Board (DSB) concluded that the United States enjoyed undisputed space dominance, thanks in large part to what the Air Force had done in the space support and force enhancement mission areas over the preceding four decades to build a thriving military space infrastructure. Air Force contributions expressly cited by the DSB included a robust space launch and support infrastructure, effective indications and warning and attack-assessment capability, unique ground-based space surveillance capability, global near-real-time surveillance of denied areas, ability to disseminate the products of that capability rapidly, and strong command, control, and communications infrastructure for exploiting space systems.[4]

In looking to build on these existing capabilities with the goal of extracting greater leverage from the military promise of space, the Air Force now faces an urgent need to prioritize its investment alternatives in an orderly and manageable way. It cannot pursue every appealing investment opportunity concurrently, since some capability upgrade needs are more pressing than others. These appropriately rank-ordered priorities, moreover, must be embraced squarely and unsentimentally by the Nation's leadership. If the experience with the successful transformation of American *airpower* since Vietnam is ever to become a prologue to the next steps in the expansion of the Nation's military space repertoire, then it follows that the Air Force, as the lead Service in space operations, will need to get its hierarchy of operational requirements in space right if near-Earth space is to be exploited for the greatest gains per cost in the service of theater commanders. Because an early working template for an overarching theory of spacepower might help impose a rational discipline on the determination of that hierarchy, perhaps the pursuit of such a focusing device should be undertaken as one of the first building blocks for such a theory.

Furthermore, a case can reasonably be made that the Nation's next moves with respect to military space exploitation should first seek to ensure the further integration of space with the needs of terrestrial warfighters, however much that might appear, at least for the near term, to shortchange the interests of those who are ready *now* to make space the fourth medium of warfare. More to the point, one can reasonably suggest that if the Nation's leadership deems a current space-based capability to be particularly important to the effective conduct of joint warfare and that it is either facing block obsolescence or otherwise is at the threshold of failing, then it should be replaced as a first order of business before any other major space investment programs are pursued. Once those most pressing recapitalization needs are attended to, then all else by way of investment opportunities can be approached in appropriate sequence, including such space-based multispectral ISR assets as electro-optical, infrared, and signals intelligence satellites, followed by space-based radar once the requisite technology has proven itself ready for major resources to be committed to it.

Moreover, in considering an orderly transfer of such ISR functions from the atmosphere to space, planners should exercise special caution not to try to change too much too quickly. For example, such legacy air-breathing systems as the E–3 Airborne Warning and Control System (AWACS) and E–8 Joint Surveillance Target Attack Radar System (JSTARS), which have been acquired through billions of dollars of investment, cannot be summarily written off with substantial service life remaining, however well intended the various arguments for mission migration to space may be. Thus, it may make greater sense to think of space not as a venue within which to replace existing surveillance functions wholesale, but rather as a medium offering the potential for expanding the Nation's existing ISR capability by more fully exploiting both the air *and* space environments. It also may help to think in terms of windows of time in which to commence the migration of ISR missions to space. A challenge that the Air Force faces now in this respect is to determine how to divest itself of existing legacy programs in a measured way so as to generate the funds needed for taking on tomorrow's challenges one manageable step at a time. That will require careful tradeoff assessments to determine the most appropriate technology and medium—air or space—toward which its resources should be vectored for any mission at any given time.

the Air Force will need to get its hierarchy of operational requirements in space right if near-Earth space is to be exploited for the greatest gains per cost

Finally, it will be essential that the survivability of any new ISR assets migrated to space be assured by appropriate protective measures developed and put into place first. American investment in appropriate first-generation space control measures has become increasingly essential in order for the Nation to remain secure in the space enabling game. Having been active in space operations for more than four decades, the United States is more heavily invested in space and more dependent on its on-orbit assets than ever before, and both real and potential adversaries are closing in on the ability to threaten our space-based assets by means ranging from harassment to neutralization to outright destruction, as attested by China's demonstration in January 2007 of a direct-ascent antisatellite kinetic kill capability against one of its own obsolete weather satellites 500 miles above the Earth's surface.[5] As the Nation places more satellites on orbit and comes to rely more on them for military applications, it is only a matter of time until our enemies become tempted to challenge our freedom of operations in space by attempting to undermine them.

In light of that fact, it would make no sense to migrate the JSTARS and AWACS

functions to space should the resultant on-orbit assets prove to be any less survivable than JSTARS and AWACS are today. It follows that getting more serious about space control is not an issue apart from force-enhancement migration, but rather represents a sine qua non for such migration. Otherwise, in transferring our asymmetric technological advantages to space, we will also run the risk of burdening ourselves with new asymmetric vulnerabilities.

Exploiting Cyberspace

If the case for proceeding with timely initiatives to ensure the continued enabling functions of the Nation's space-based assets sounds reasonable enough in principle, then the argument for pursuing similar measures by way of vouchsafing our continued freedom of movement in cyberspace can be said to be downright compelling. The latter arena, far more than today's military space environment, is one in which the Nation faces clear and present threats that could be completely debilitating when it comes to conducting effective military operations. Not only that, opponents who would exploit opportunities in cyberspace with hostile intent have every possibility for adversely affecting the very livelihood of the Nation, since that arena has increasingly become not just the global connective tissue, but also the Nation's central nervous system and center of gravity.

Just a few generations ago, any American loss of unimpeded access to cyberspace would have been mainly an inconvenience. Today, however, given the Nation's ever-expanding dependence on that medium, the isolation, corruption, or elimination of electrical power supply, financial transactions, key communications links, and other essential Web-based functions could bring life as we know it to a halt. Furthermore, given the unprecedented reliance of the United States today on computers and the Internet, cyberspace has arguably become the Nation's center of gravity not just for military operations, but for *all* aspects of national activity, to include economic, financial, diplomatic, and other transactions. Our heightened vulnerability in this arena stems from the fact that we have moved beyond the era of physical information and financial exchanges through paper and hard currency and rely instead on the movement of digital representations of information and wealth. By one informed account, more than 90 percent of American business in all sectors, to say nothing of key institutions of governance and national defense, connects and conducts essential communications within the cyberspace arena.[6] Accordingly, that arena has become an American Achilles' heel to a greater extent than for any of our current opponents.

The term *cyberspace* derives from the Greek word *kubernetes*, or "steersman." Reduced to basics, it is the proverbial ether within and through which electromagnetic radiation is propagated in connection with the operation and control of mechanical and electronic transmission systems. Properly understood, cyberspace is not a "mission," but rather an operating domain just like the atmosphere and space, and it embraces all systems that incorporate software as a key element. It is a medium, moreover, in which information can be created and acted on at any time, anywhere, and by essentially anyone. It is qualitatively different from the land, sea, air, and space domains, yet it both overlaps and continuously operates within all four. It also is the only domain in which all instruments of national power (diplomatic, informational, military, and economic) can be concurrently exercised through the manipulation of data and gateways. Cyberspace can be thought of as a "digital commons" analogous to the more familiar maritime, aerial, and exoatmospheric commons. Moreover, just like the other three commons, it is one in which our continued uninhibited access can never be taken for granted as a natural and assured right. Yet uniquely among the other three, it is a domain in which the classic constraints of distance, space, time, and investment are reduced, in some cases dramatically, both for ourselves and for potential enemies.

There is nothing new in principle about cyberspace as a military operating domain. On the contrary, it has existed for as long as radio frequency emanations have been a routine part of military operations. As far back as the late 1970s, the commander in chief of the Soviet navy, Admiral Sergei Gorshkov, declared famously that "the next war will be won by the country that is able to exploit the electromagnetic spectrum to the fullest."[7] Furthermore, the Soviets for decades expounded repeatedly, and with considerable sophistication and seriousness, on a mission area that they referred to as *REB* (for *radioelektronaya bor'ba*, or radio-electronic combat). However, only more recently has it been explicitly recognized as an operating arena on a par with the atmosphere and space and begun to be systematically explored as a medium of combat in and of itself.

At present, theorizing about airpower and its uses and limitations has the most deeply rooted tradition in the United States, with conceptualizing about military space occupying second place in that regard. In contrast, focused thinking about operations in cyberspace remains in its infancy. Yet cyberspace-related threats to American interests are currently at hand to a degree that potentially catastrophic air and space threats are not—at least yet. Accordingly, the U.S. defense establishment should have every incentive to get serious about this domain now, when new terrorist, fourth-generation warfare, and information operations challengers have increasingly moved to the forefront alongside traditional peer-adversary threats.[8]

In light of that emergent reality, it is essential to include cyberspace in any consideration of air and space capabilities. Like the air and space domains, cyberspace is part and parcel of the third dimension (the first two being the land and maritime environments). Also like those other two domains, it is a setting in which organized attacks on critical infrastructure and other targets of interest can be conducted from a distance, on a wide variety of "fronts," and on a global scale—except, in this case, at the speed of light. Moreover, it is the principal domain in which the Nation's air services exercise their command, control, communications, and ISR capabilities that enable global mobility and rapid long-range strike.

In thinking about cyberspace as a military operating arena, a number of the medium's distinguishing characteristics are worth noting. First and foremost, control of cyberspace is a sine qua non for operating effectively in the other two domains. Were unimpeded access to the electromagnetic spectrum denied to us through hostile actions, satellite-aided munitions would become useless, command and control mechanisms would be disrupted, and the ensuing effects could be paralyzing. Accordingly, cyberspace has become an emergent theater of operations that will almost surely be contested in any future fight. Successful exploitation of this domain through network warfare operations can allow an opponent to dominate or hold at risk any or all of the global commons. For that reason, not only American superiority but also American dominance must be assured.

B–2 Spirit stealth bomber lands at Nellis Air Force Base, Nevada, after completing mission during exercise Red Flag

U.S. Air Force (Thomas P. Dougherty)

One reason for the imminent and broad-based nature of the cyberspace challenge is the low buy-in cost compared to the vastly more complex and expensive appurtenances of air and space warfare, along with the growing ability of present and prospective Lilliputian adversaries to generate what one expert called "catastrophic cascading effects" through asymmetric operations against the American Gulliver.[9] Because the price of entry is fairly minimal compared to the massive investments that would be required for any competitor to prevail in the air and space domains, the cyberspace warfare arena naturally favors the offense. It does so, moreover, not only for us, but also for any opponents who might use the medium for conducting organized attacks on critical nodes of the Nation's infrastructure. Such attacks can be conducted both instantaneously and from a safe haven anywhere in the world, with every possibility of achieving high impact and a low likelihood of attribution and, accordingly, of timely and effective U.S. retribution.

Indeed, America's vulnerabilities in cyberspace are open to the entire world and are accessible to anyone with the wherewithal and determination to exploit them. Without appropriate defensive firewalls and countermeasures in place, anything we might do to exploit cyberspace can be done to us as well, and relatively inexpensively. Worse yet, threat trends and possibilities in the cyberspace domain put in immediate jeopardy much, if not all, of what the Nation has accomplished in the other two domains in recent decades. Our continued prevalence in cyberspace can help ensure our prevalence in combat operations both within and beyond the atmosphere, which, in turn, will enable our prevalence in overall joint and combined battlespace. On the other side of the coin, any loss of cyberspace dominance on our part can negate our most cherished gains in air and space in virtually an instant. Technologies that can enable offensive cyberspace operations, moreover, are evolving not only within the most well-endowed military establishments around the world, but even more in the various innovative activities now under way in other government, private sector, and academic settings. The United States commands no natural advantage in this domain, and our leaders cannot assume that the next breakthrough will always be ours. All of this has rendered offensive cyberspace operations an attractive asymmetric option not only for mainstream opponents and other potential exploiters of the medium in ways inimical to the Nation's interests, but also for state and nonstate rogue actors with sufficient resources to cause us real harm.

Moreover, unlike the air and space environments, cyberspace is the *only* military operating area in which the United States already has peer competitors in place and hard at work. As for specific challengers, U.S. officials have recently suggested that the most sophisticated threat may come from China, which unquestionably is already a peer competitor with ample financial resources and technological expertise. There is more than tangential evidence to suggest that cyberwar specialists in China's People's Liberation Army have already focused hostile efforts against nonsecure U.S. transmissions.[10] Such evidence bears strong witness to the fact that state-sponsored cyberspace intrusion is now an established fact and that accurate and timely attack characterization has come to present a major challenge.

In light of its relative newness as a recognized and well-understood medium of combat, detailed and validated concepts of operations for offensive and defensive counter–cyber warfare and cyberspace interdiction have most likely yet to be worked out and formally incorporated into the Nation's combat repertoire. Interestingly, some of the most promising initial tactical insights toward that end may come from accessible sources in the nonmilitary domain, including from the business world, the intelligence world, the high-end amateur hacker world, and even perhaps segments of the underworld that have already pioneered the malicious exploitation of cyberspace. Ultimately, such efforts can help inform the development of a full-fledged theory of cyberspace power, which, at bottom, "is about dominating the electromagnetic spectrum—from wired and unwired networks to radio waves, microwaves, infrared, x-rays, and directed energy."[11]

With a full-court press of creative thought toward the development of new capabilities, the possibility of what a future cyberspace weapons array might include is almost limitless. Cyber weapons can be both surgical and mass-based in their intended effects,

ranging from what one Air Force cyber warrior recently portrayed as "the ultimate precision weapon—the electron," all the way to measures aimed at causing mass disruption and full system breakdowns by means of both enabling and direct attacks.[12] The first and most important step toward dealing effectively with the cyberspace warfare challenge in both threat categories will be erecting impenetrable firewalls for ourselves and taking down those of the enemy. Of course, with respect to plausible techniques and procedures for tomorrow's cyberspace world, it will be essential never to lose sight of the timeless rule among airmen that a tactic tried twice is no longer a tactic but a procedure.

cyberspace warfare professionals will need to learn that any "cyberspace culture" must not be isolated from mainstream combat forces in all Services

As the newly emerging cyberspace warfare community increasingly sets its sights on such goals, it would do well to consider taking a page from the recent experience of the military space community in charting next steps by way of organizational and implementation measures. For example, just as the military space community eventually emulated to good effect many conventions of the air warfare community, so might the cyberspace community usefully study the proven best practices of the space community in gaining increased relevance in the joint warfare world. Some possible first steps toward that end might include a systematic stocktaking of the Nation's cyberspace warfare posture with a view toward identifying gaps, shortfalls, and redundancies in existing offensive and defensive capabilities.

Similarly, those now tasked with developing and validating cyberspace concepts of operations might find great value in reflecting on the many parallels between space and cyberspace as domains of offensive and defensive activity. For example, both domains, at least today, are principally about collecting and transmitting information. Both play pivotal roles in enabling and facilitating lethal combat operations by other force elements. Both, again at least today, have more to do with the pursuit of functional effects than with the physical destruction of enemy equities, even though both can materially aid in the accomplishment of the latter. Moreover, in both domains, operations are conducted remotely by warfighters sitting before consoles and keyboards, not only outside the medium itself, but also in almost every case out of harm's way. Both domains are global rather than regional in their breadth of coverage and operational impact. And both domains overlap—for example, the jamming of a GPS signal to a satellite-aided munition guiding to a target is both a counterspace and a cyberwar operation insofar as the desired effect is sought simultaneously in both combat arenas.[13] To that extent, it seems reasonable to suggest that at least some tactics, techniques, procedures, and rules of thumb that have been found useful by military space professionals might also offer promising points of departure from which to explore comparable ways of exploiting the cyberspace medium.

Finally, as cyberspace professionals become more conversant with the operational imperatives of joint warfighting, they also will have a collective obligation to rise above the fragmented subcultures that unfortunately still persist within their *own* community and become a more coherent and interconnected center of cyberspace excellence able to speak credibly about what the exploitation of that medium brings to joint force employment. Moreover, cyberspace warfare professionals will need to learn and accept as gospel that any "cyberspace culture" that may ultimately emerge from such efforts must not be isolated from mainstream combat forces in all Services, as the Air Force's space sector was when it was in the clutches of the systems and acquisition communities, but instead must be rooted from the start in an unerring focus on the art and conduct of war.

Toward Synthesis

As long as military space activity remains limited to enabling rather than actually conducting combat operations, as will continue to be the case for at least the near-term future, it will arguably remain premature even to *think* of the notion of space "power," strictly speaking, let alone suggest that the time has come to begin crafting a self-standing theory of spacepower comparable in ambitiousness and scope to the competing (and still-evolving) theories of land, sea-, and airpower that were developed over the course of the 20th century. Only when desired operational effects can be achieved by means of imposition options exercised directly through and from space to space-based, air-breathing, and terrestrial targets of interest (or, more to the point, when we can directly inflict harm on our adversaries from space) will it become defensible to entertain thoughts about space "power" as a fact of life rather than as merely a prospective and desirable goal.

To be sure, it scarcely follows from this observation that today's space professionals have no choice but to wait patiently for the day when they become force appliers on a par with their air, land, and maritime power contemporaries before they can legitimately claim that they are true warfighters. On the contrary, the Nation's space capabilities have long since matured to a point where they have become just as important a contributor to the overall *national* power equation as has what one might call mobility power, information power, and all other such adjuncts of the Nation's military strength that are indispensable to joint force commanders for achieving desired effects at all levels of warfare. To that extent, insisting that it remains premature to speak of spacepower solely because our space assets cannot yet deliver such combat effects directly may, in the end, be little more than an exercise in word play when one considers what space already has done toward transforming the Nation's airpower into something vastly more capable than it ever was before U.S. on-orbit equities had attained their current breadth of enabling potential.

Until the day comes when military space activity is more than "merely" about enabling terrestrial combat operations, however, a more useful exercise in theory-building in the service of combat operators at all levels might be to move beyond the *air*-power theorizing that has taken place to date in pursuit of something akin to a working "unified field theory" that explicates the connections, interactions, and overlaps among the air, space, and cyberspace domains in quest of synergies between and among them in the interest of achieving a joint force commander's objectives more efficiently and effectively. A major pitfall to be avoided in this regard is the pursuit of separate theory sets for each medium. To borrow from Clausewitz on this point, space, like the Earth's atmosphere and electromagnetic spectrum, may have its own grammar, but it does not have its own logic. Each of the three environments explored in the preceding

pages has distinctive physical features and operating rules that demand respect. By one characterization in this regard, "air permits freedom of movement not possible on land or sea.... Space yields an overarching capability to view globally and attack with precision from the orbital perspective. Cyberspace provides the capability to conduct combat on a global scale simultaneously on a virtually infinite number of 'fronts.'"[14] Yet while the air, space, and cyberspace mediums are all separate and unique physical environments, taken together, they present a common warfighting challenge in that operations in each are mutually supportive of those in the other two. For example, the pursuit of air supremacy does not simply entail combat operations in the atmosphere, but also hinges critically on ISR functions and on GPS targeting from both air-breathing and space-based platforms that transmit through cyberspace.

In light of the foregoing, the most immediate task for those seeking to build a better theory for leveraging capabilities in the third dimension may be to develop a point of departure for thinking systematically and holistically about synergies and best uses of the Nation's capabilities and prospects in all three domains, since all are key to the Nation's transforming joint strike warfare repertoire. Furthermore, it would be helpful to have a seamless body of applied and actionable theory that encompasses all three domains and that focuses more on functions and effects than on the physical locations of the instruments of power, with a view toward rank-ordering the many priorities in each and across all three, with the goal of charting a course for achieving cross-domain dominance. Another useful step toward managing the existing seams between and among the air, space, and cyberspace communities within the American defense establishment would be a perspective focused on *operational integration* accompanied by *organizational differentiation*. Through such a bifurcated approach, each medium can be harnessed to serve the needs of all components in the joint arena while, at the same time, being treated rightly as its own domain when it comes to program and infrastructure management, funding, cadre building, and career development.[15] Such organizational differentiation will be essential for the orderly growth of core competencies, discrete career fields, and mature professionalism in each medium. However, operational integration should be the abiding concern and goal for all three mediums, since it is only from synergies among the three that each can work to its best and highest use.

This is *not* a call for the Air Force, as the Nation's main repository of air, space, and cyberspace warfare capabilities today, to make the same mistake in a new guise that it made in 1959 when it conjured up the false artifice of "aerospace" to suggest that the air and space mediums were somehow undifferentiated just because they happened to be coextensive. Nothing could be further from the truth. It is, rather, to spotlight the unifying purpose of operations in all three mediums working in harmony, namely, to deliver desired combat effects in, through, and from the third dimension as quickly as possible and at the least possible cost in friendly lives lost and unintended damage incurred. Only after that crucial transitional stage of conceptualization has passed and when military space operations have come into their own as an independent producer, rather than just an enabler, of combat effects will it be possible to start giving serious thought to coming to grips with the prerequisites for a self-standing theory of spacepower. **JFQ**

NOTES

[1] For an overview of the Air Force's pivotal contribution to this transformation, see Benjamin S. Lambeth, "The Air Force Renaissance," in *The Air Force*, ed. James P. McCarthy and Drue L. DeBerry (Andrews Air Force Base, MD: The Air Force Historical Foundation, 2002), 190–217. A fuller assessment of post-Vietnam developments in fixed-wing air warfare capability in all of the Services may be found in Benjamin S. Lambeth, *The Transformation of American Airpower* (Ithaca, NY: Cornell University Press, 2000).

[2] These major air operations are examined in detail in Benjamin S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND Corporation, 2001); *Airpower Against Terror: America's Conduct of Operation* Enduring Freedom (Santa Monica, CA: RAND Corporation, 2005); and *The Unseen War: Airpower in the Major Combat Phase of Operation Iraqi Freedom* (Santa Monica, CA: RAND Corporation, forthcoming).

[3] Of course, space plays a larger role in the "fixing" of targets than just providing space-based ISR. Space-based communications and the Global Positioning System are both essential enablers of unmanned aerial vehicle operations, which are also a critical contributor to the "find, fix, track, target, engage, assess" equation.

[4] Cited in E.C. Aldridge, Jr., "Thoughts on the Management of National Security Space Activities of the Department of Defense," unpublished paper, July 6, 2000, 3.

[5] For the essential known details of the test, see Craig Covault, "Space Control: Chinese Antisatellite Weapon Test Will Intensify Funding and Global Policy Debate on the Military Uses of Space," *Aviation Week and Space Technology*, January 22, 2007, 24–25.

[6] General James Cartwright, USMC, Commander, U.S. Strategic Command, remarks at the Air Force Association's Warfare Symposium, Orlando, Florida, February 8, 2007.

[7] Sergei G. Gorshkov, *The Sea Power of the State* (Annapolis, MD: Naval Institute Press, 1979).

[8] Among the classic articles in the airpower theory literature are Edward Warner, "Douhet, Mitchell, Seversky: Theories of Air Warfare," in *Makers of Modern Strategy*, ed. Edward Mead Earle (Princeton: Princeton University Press, 1943), and David MacIsaac, "Voices from the Central Blue: The Airpower Theorists," in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton: Princeton University Press, 1986). See also the collection of essays in Phillip S. Meilinger, ed., *The Paths of Heaven: The Evolution of Airpower Theory* (Maxwell Air Force Base, AL: Air University Press, 1997). One of the better synopses of spacepower thinking to date is presented in Peter L. Hays et al., *Spacepower for a New Millennium: Space and U.S. National Security* (New York: McGraw Hill, 2000). For the most serious and thorough treatise thus far to have expounded about the cyberspace domain, its boundaries, and its potential, see George J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001). The book is the doctoral dissertation of an Air Force lieutenant colonel who commanded the 23d Information Operations Squadron in the Air Force Information Warfare Center.

[9] Colonel Glenn Zimmerman, USAF, "The United States Air Force and Cyberspace: Ultimate Warfighting Domain and the USAF's Destiny," unpublished paper.

[10] See Carlo Munoz, "Air Force Official Sees China as Biggest U.S. Threat in Cyberspace," *Inside the Air Force*, November 17, 2006.

[11] "Ten Propositions Regarding Cyber Power," Air Force Cyberspace Task Force, unpublished briefing chart, no date.

[12] Zimmerman.

[13] I am grateful to my RAND colleague Karl Mueller for suggesting these and other thought-provoking parallels between the two media.

[14] Zimmerman.

[15] For an earlier development of this line of argument with respect to the Air Force's space community, see Benjamin S. Lambeth, *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space* (Santa Monica, CA: RAND Corporation, 2003).