Multidomain Operations

A Subtle but Significant Transition in Military Thought

Dr. Jeffrey M. Reilly

Disclaimer: The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

On 17 November 2011, Gen Martin Dempsey, chairman of the Joint Chiefs of Staff, asked the Military Education Coordination Council the prophetic question, "What's after joint?"[1] After more than four years, that question remains ostensibly unanswered. The answer, however, may reside in the notion of multidomain operations.[2] General Dempsey's inquiry was spurred by the fact that historical approaches to achieving superiority in the air, land, and sea domains may no longer be valid. The principal factor driving this phenomenon is a global proliferation of advanced information technology. Although the United States has undergone dramatic changes in technology in the past, we are in only the nascent stages of understanding this era's monumental impact on future military operations. The worldwide flood of powerful, inexpensive, and readily available commercial technology is mandating a much more sophisticated approach to military affairs. The primary catalyst for this revolution has been the miniaturization of the transistor. In 1965 Gordon Moore observed that the number of transistors on integrated circuits doubles approximately every two years.[3] Transistors control the flow of electricity in a circuit, and the miniaturization of the transistor has enabled 20 billion of them to be emplaced on single wafer-thin computer chips no bigger than a fingernail.[4] Consequently, computer processing power has been doubling every two years and is expected to continue to the year 2020.[5] The exponential growth associated with Moore's Law has created a security environment where the pace of cyber, directed energy, nanotechnology, robotics, and biotechnology advancements is far beyond the normal capacity to predict their effects. Advanced information technology is also changing our perspectives of multidomain interdependence. America's ability to project conventional power abroad is eroding swiftly as state and nonstate actors acquire advanced capabilities to offset the US military's strengths across all operating domains—air, land, sea, space, and cyberspace.[6] Additionally, the requirement to think across domains is occurring at increasingly lower levels and will be essential in the future to generating the tempo critical to exploiting fleeting local opportunities for disrupting an enemy system.[7] These changes in the operational environment, combined with "new" fiscal realities, are rapidly transforming how we need to think about threats, the battlespace, and the conceptual underpinnings of airpower.

Multidomain Operations Are an Enduring Characteristic of Warfare

The concept of cross-domain operations is not new. It has been an inherent part of military thought since antiquity. The disastrous Athenian campaign to conquer Sicily during the Peloponnesian War provides just one example (fig. 1). In 415 BC, Athens launched an ill-advised expedition to subdue Sicily's strongest state, Syracuse. The Athenian force led by Nicias consisted of approximately 6,400 men and 134 ships. The Athenians enjoyed early successes; however, in 414 BC during the siege of Syracuse, the Spartan strategos Gylippus intervened and turned the tide of battle in favor of the Syracusan forces. Gylippus focused initially on the human domain, inspiring the Syracusan forces and galvanizing the support of their allies. He then embarked upon simultaneous attacks of the Athenian troops on the land and at sea. By 413 BC, the Athenians had been defeated.[8]

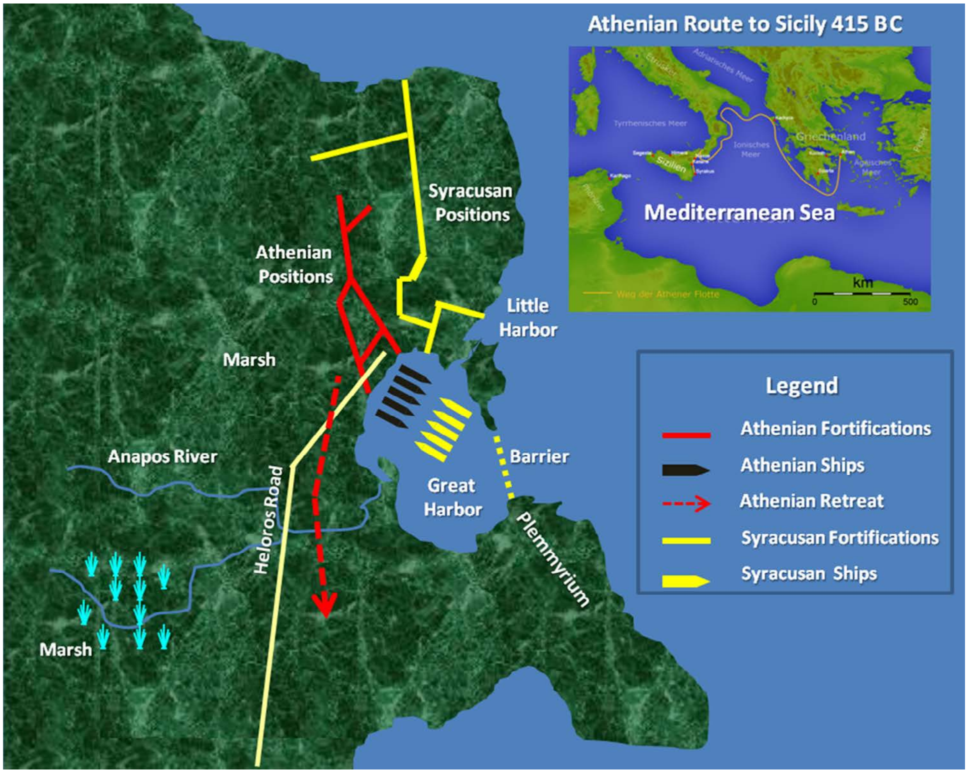

Figure 1. Athenian debacle in Sicily

This defeat signaled the beginning of the end for the Athenian empire. It created panic in Athens, caused a major shift in Athenian alliances, and paved the way for Sparta's final victory over Athens in 404 BC. However, the lesson of this historical example goes far beyond the collapse of Athens. It highlights the importance of understanding multiple domains and the necessity of shifting local superiority between domains. Gylippus and the Syracusan forces were not successful in all of their engagements. In fact, the Athenians defeated or repelled those forces at several key points in the campaign. Nevertheless, Gylippus concentrated on what is now becoming a crucial idea embedded in the Joint Operational Access Concept—specifically, that superiority in any domain may not be widespread or permanent but more often local and temporary.[9] Gylippus's comprehension of linking multiple domains and operating across domains was the intrinsic element in Syracuse's victory. The lesson from Gylippus is that establishing superiority in a combination of domains offers the freedom of action necessary to attain mission success.

Challenges of Future Technological Threats

As the US military embarks upon the chairman's Capstone Concept for Joint Operations, the emerging strategic landscape is revealing a wide array of new threats that is dramatically degrading the overwhelming asymmetric advantage we have enjoyed for the past two decades. Unable to compete with US forces directly, adversaries are leveraging technological advances to create their own asymmetric advantages in countering US military superiority.[10] Russia, Iran, North Korea, and China have invested in a number of ballistic and supersonic cruise missiles designed to challenge the United States' conventional superiority. China's DF-21D, a medium-range ballistic missile, reportedly possesses a maneuverable reentry vehicle, features terminal guidance based upon both the Global Positioning System and active radar, and can strike 1,500 to 2,000 kilometers (km) away from China's shores (fig. 2).[11]

At least nine countries are involved in the development and production of land attack cruise missiles, and many of these weapons will be available for export within the next decade.[12] Innovations in cruise missile technology have created supersonic threats that can engage targets 300 km away and be delivered by a variety of systems such as aircraft, submarines, ships, or even trucks.[13] Furthermore, modern cruise missiles can be programmed to approach and attack a target in the most efficient manner, allowing an adversary to fire multiple missiles and strike simultaneously from different directions, overwhelming air defenses at their weakest points.[14] Newer missiles are incorporating stealth features to make them even less visible to radars and infrared detectors, and they can be armed with conventional, air-fuel, or even low-yield nuclear warheads.[15]

In addition to threats from advanced missile technology, between 2004 and 2012, the number of countries having acquired remotely piloted vehicles increased from 41 to at least 76.[16] Many of them are seeking to enhance not only their intelligence acquisition but also armed strike capabilities.

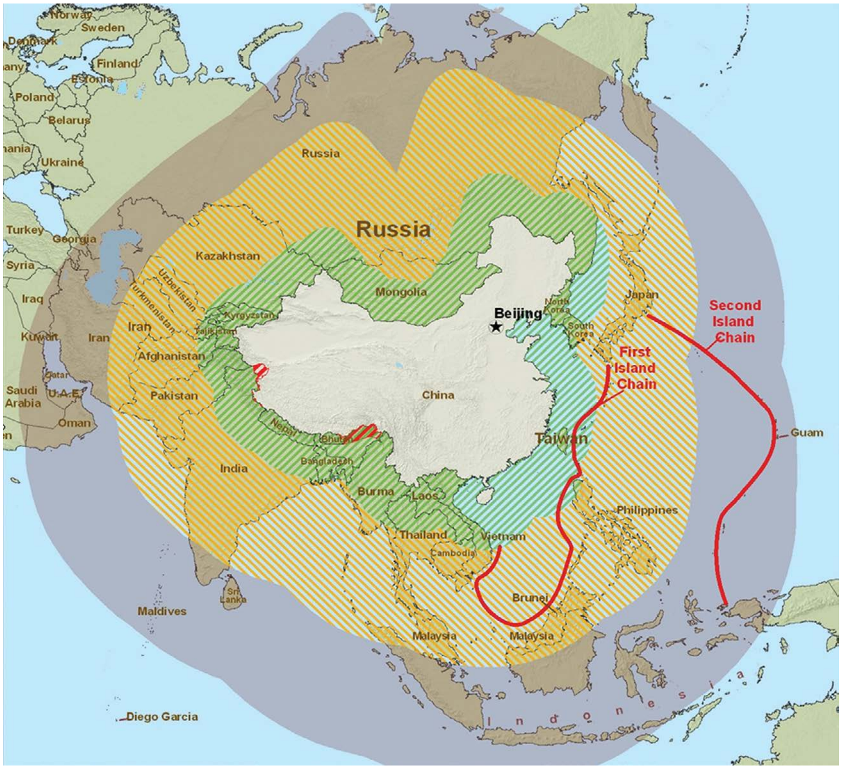

Figure 2. Conventional antiaccess missile capabilities of the People's Republic of China. (Reprinted from Department of Defense, Office of the Secretary of Defense, *Military Power of the People's Republic of China: A Report to Congress pursuant to the National Defense Authorization Act, Fiscal Year 2000* [Washington, DC: Department of Defense, Office of the Secretary of Defense, 2009], 23.)

Furthermore, numerous countries are working on high-powered microwave (HPM), directed-energy, and electromagnetic pulse (EMP) weapons (fig. 3). A 2005 declassified intelligence report on the bio-effects of Chinese EMP and HPM weapons indicated that China could detonate a low-yield, low-altitude strategic nuclear warhead to destroy electronic systems while minimizing the effects to the Chinese mainland.[17] The significance of this intelligence is that it sheds light on using weapons systems to deny multiple domains simultaneously. EMP damages unhardened electrical circuits and electronics by generating a surge in the current and voltage beyond normal functioning capacity. A 1-megaton nuclear blast detonated 400 km above the center of the United States can have continental-wide terrestrial effects in seconds, as well as a significant impact on space capabilities.[18] Take, for example, the United States' 1962 "Starfish Prime" nuclear test when a 1.4 megaton weapon was detonated 400 km above the earth's surface. The electromagnetic effects from the detonation not only reached Hawaii, 898 miles away, but also created an intense artificial radiation belt that began damaging orbiting weather and communications satellites. The artificial radiation belt destroyed seven satellites and persisted until the early 1970s.[19] To place this in perspective, over 40 percent of the world's active satellites are in low Earth orbit. One should also note that adversaries can deliver effects from EMP through a multitude of nonnuclear modes that produce a wide array of outcomes ranging from temporary interference to system destruction. These modes include ballistic missiles, submarines, aircraft, and satellites as well as man-packed systems such as an explosively pumped flux compression generator.[20]

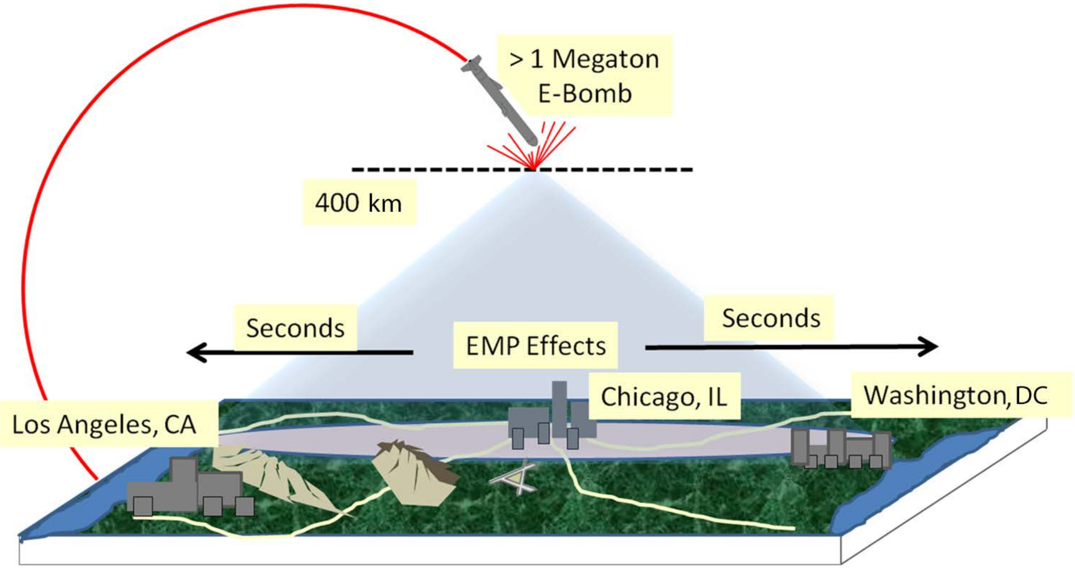

Figure 3. Effects of electromagnetic pulse. (Derived from Headquarters Department of the US Army, *Nuclear Environment Survivability* [US Army White Sands Missile Range, NM: US Army Test and Evaluation Command, 15 April 1994], appendix D.)

Advances in technology are also affecting an adversary's ability to defend itself. Integrated air defense systems are becoming increasingly resistant to electronic suppression through the use of passive sensor technologies such as infrared search and track. These technology leaps are being augmented with surface-to-air missiles that have advanced tracking and longer ranges. Potential adversaries are also investing in inexpensive low-power jammers to inhibit the positioning, navigation, and timing necessary for effective strike operations.[21]

Changes in Adversarial Concepts and Strategies

Although the military modernization of possible enemies is disconcerting, it is only part of the future threat equation. Prospective foes are combining advances in technology with operational concepts and strategies designed to deny the US military asymmetric maneuver in multiple domains. The People's Republic of China (PRC) is aggressively pursuing this path, combining what it refers to as *shashoujian* (trump card or assassin's mace) technology with the concept of unrestricted warfare and an information warfare strategy. *Shashoujian* refers to a set of military capabilities that enables the technologically inferior to defeat the technologically superior. These capabilities include advanced integrated air defense systems, ballistic and cruise missiles, advanced strike aircraft, attack submarines, and counterspace capabilities.[22] A number of Chinese authors advocate going beyond the traditional boundaries of warfare, when necessary, to realize national political objectives. They propose using *shashoujian* strikes on a superior adversary's critical nodes to paralyze his forces and cause disintegration.[23] The following excerpt from Col Qiao Liang and Col Wang Xiangsui's book *Unrestricted Warfare* provides exceptionally sobering insight into the conceptual underpinnings of *shashoujian* and the concept of unrestricted warfare:

> Supposing a war broke out between two developed nations already possessing full information technology, and relying upon traditional methods of operation, the attacking side would generally employ the modes of great depth, wide front, high strength, and three-dimensionality to launch a campaign assault against the enemy. . . . However, by using the combination method, a completely different scenario and game can occur: if the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty.[24]

The recent exposure of the People's Liberation Army (PLA) Unit 61398 in Shanghai by the Mandiant cybersecurity firm highlights the PRC's ability and willingness to conduct cyber exploitation and cyber attack operations globally.[25] The PRC's well-publicized cyber capabilities go far beyond collecting and exploiting intelligence data. The difference between cyber exploitation and attack is as simple as a keystroke. The PLA is actively creating the strategic guidance, tools, and trained personnel necessary to employ computer network operations in support of traditional war-fighting disciplines.[26] Cyberspace offers the PRC and other state and nonstate actors the capacity to delay an adversary's response to a kinetic attack by implanting malicious code in advance on the enemy's logistics; command, control, communications, computers, intelligence, surveillance, and reconnaissance; and commercial support networks.[27]

In spite of the significant advantages that China enjoys from cyberspace, it is not the focal point of the PRC's information warfare strategy. The PLA's assessments of current and future conflicts note that campaigns will be conducted in all domains simultaneously but that its emphasis on the electromagnetic spectrum has driven the PLA to adopt a much more comprehensive approach.[28] In 2002 the PLA's Maj Gen Dai Qingmin characterized electronic warfare as an intangible power necessary for success. He pointed out that whichever side loses in an electronic war will be reduced to blindness and deafness, so its weapons will be disabled, and it will lose its initiative in a battle, campaign, or even an entire strategic situation.[29] PRC writings emphasize that electromagnetic dominance in the early phases of a campaign is one of the foremost tasks to ensure battlefield success. The Chinese strategy known as integrated network electronic warfare combines electronic warfare, computer network operations, and kinetic strikes to disrupt battlefield information systems that support an adversary's war-fighting and power-projection capabilities. This type of warfare also stresses that the electromagnetic spectrum is a vital fourth dimension equally as important as traditional ground, sea, and air forces.[30]

China's military modernization and strategy are a harbinger of a broader trend in which smaller regional powers and even nonstate actors are seeking to develop or procure asymmetric capabilities that are changing the traditional notion of military operations.[31] For the United States, the implications of this phenomenon are numerous and serious enough to mandate another look at how we educate future Air Force leaders to develop, coordinate, and execute air operations. One of the most dynamic implications is the shift in conceptualization of the battlespace and its impact on the homeland, space, and the electromagnetic spectrum.

Implications for the Concept of the Battlespace

Advances in technology have subtly nudged the entire globe into a realm where all previous notions of the battlespace have been radically altered by domain interdependence driven by a combination of factors ranging from advanced technology efficiency to fiscal constraints. These factors are creating an environment where failure in one domain has cascading effects in one or more of the others. Postmodern technology is quickly fusing a continuum of integrated and interdependent domains. Figure 4 provides a simplistic illustration of this continuum. In this construct, the electromagnetic spectrum (EMS) empowers space, allowing it to supply key enablers for the domains of air, land, and sea, in turn facilitating the ability to influence or control the human domain. Hypothetically, if an opponent attacks or manipulates the use of radio frequencies within the EMS, through cyber or other means, he could deny access to vital satellites that we rely on for intelligence, surveillance, and reconnaissance; communications; early warning; and navigation. The consequences would severely affect a joint force air component commander's planning, decision, and execution cycle and could render operations in the air, on land, and at sea ineffective. Future Airmen must be sufficiently cognizant of this integrated operational environment to ensure that enough local superiority in the right combination of domains fosters the conditions necessary for operational success.

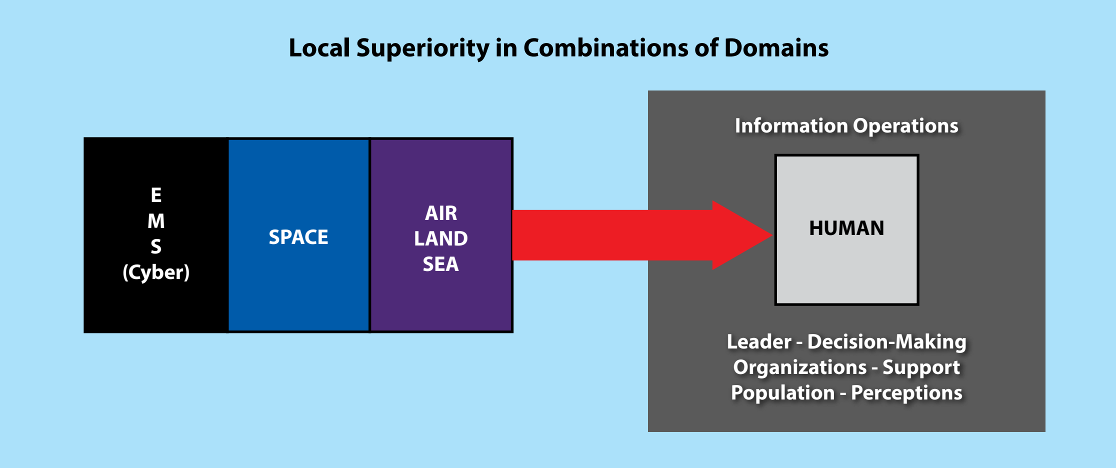

Figure 4. Continuum of domains and their interdependence

It is also important to emphasize that the transformation of the battlespace is much more significant than challenges related to operating in a highly contested EMS within a designated joint operations area. For the first time since the end of the Cold War, the United States faces the threat of a catastrophic attack on the homeland beyond the scale of the terrorist strikes of 11 September 2001. The historical barriers of the Atlantic and Pacific oceans are no longer effective means to negate an enemy's operational reach. The simple arrangement of 1s and 0s traveling at the speed of light can transmit computer packets of information to US homeland systems via a radio frequency signal almost instantaneously. Furthermore, these information packets can be pre-positioned and lay dormant within systems well prior to any attack without prior detection. The continuing growth of networked systems, devices, and platforms offers prospective state and nonstate foes a plethora of vulnerabilities to threaten US national security that go well beyond military targets. The integrated nature of cyberspace in the realm of power grids, transportation networks, communications, and financial systems represents a lucrative target that would allow an adversary to cause massive physical damage and economic disruption to the US homeland.

Since 2006 the unauthorized access to and installation of malicious software on US government computers have increased by 650 percent.[32] Moreover, the Department of Homeland Security reported 198 cyber attacks on critical US infrastructure during 2012—a 52 percent increase over those that occurred in 2011.[33] A five-year-old National Academy of Sciences report, declassified and released in November 2012, found that physical damage by terrorists to large transformers could disrupt power to large regions of the country and could take months to repair.[34] Furthermore, this type of attack could be carried out with little risk of detection or interdiction. As a reference point, the largest power blackout in North American history took place on 14 August 2003 when four sagging high-voltage power lines in northern Ohio brushed into some trees. A computer system error further complicated the accident.[35] This incident left 50 million people across the United States and Canada without power, cost $6 billion to repair, and may have contributed to 11 deaths. Given this example, it is not hard to imagine a determined adversary simultaneously attacking combinations of critical infrastructures such as the electric grid, pipelines, communications, transportation, and financial networks. The devastation would be incalculable. In his book *America the Vulnerable*, Joel Brenner estimates that it would take two years to replace the heavy-duty generators that supply electricity to large cities.[36]

Another significant change in battlespace is space. Since 1991 the United States has become more reliant on space-based capabilities to support military operations. Space assets provide the means to communicate globally; conduct the positioning, navigation, and timing necessary for precision strikes; and empower enhanced intelligence, surveillance, and reconnaissance. Further, space furnishes virtually unimpeded overflight access to conduct the monitoring essential for missile-launch detection, missile tracking, and early warning. Opponents clearly recognize space's intrinsic role as a US force multiplier, and they also possess an understanding of its considerable vulnerabilities.

A satellite system consists of three basic components: the satellite itself, the ground stations used to command and control it, and the communication links between the components. All of the latter have varying degrees of vulnerabilities. Satellites themselves are nearly impossible to hide. They move along predictable paths, are visible to observers over large swaths of the earth, and can appreciably change their orbit only with significant effort. Adversaries can employ a variety of attack options, including kinetically striking the ground stations, jamming or spoofing links, and using directed energy to dazzle or partially blind the satellite. On a more revolutionary level, future enemies could theoretically use "parasitic microsatellites" that could latch onto a satellite and disable it, alter its orbit, or hijack the information gathered by it.[37]

The principal concern today is the rapid acceleration of the militarization and weaponization of space. On 11 January 2007, the PRC conducted its first successful direct-ascent antisatellite weapons test, launching a ballistic missile armed with a kinetic-kill vehicle to destroy the Fengyun-1C weather satellite at about 530 miles up in low Earth orbit.[38] China followed up in 2010 and 2013 with additional antisatellite tests. On 13 May 2013, it fired a missile into space that reached an altitude of over 6,000 miles and possibly over 20,000 miles.[39] This range could allow China to attack US Global Positioning System and military and intelligence satellites in medium and high Earth orbits. Antisatellite missiles, however, are far from the only threat to the US military's use of space. Space-based capabilities are dependent upon the EMS for effective operations since it provides the sole medium for transmitting and receiving information and signals in space.[40] Additionally, the frequency bands that space-based systems use within the spectrum are fixed and cannot be changed after launch.

The EMS is a physics-based maneuver space that is essential to control the operational environment during all military operations.[41] The spectrum represents the range of wavelengths or frequencies over which electromagnetic radiation extends. It encompasses the use of electromagnetic radiation associated with radio, microwave, infrared, visible, ultraviolet, X-rays, and gamma rays, exerting a dominant influence on all domains. The EMS is crucial for communications, command and control, blue force tracking, precision attack, and a host of other joint functions used every day and commonly taken for granted. Furthermore, the Department of Defense has invested billions of dollars in developing, maintaining, and employing war-fighting capabilities that rely on access to the EMS.[42] The projected investment for the development and procurement of fixed-wing airborne electronic attack systems alone in 2007–16 is more than $17.6 billion.[43]

Like space, the EMS is exceedingly complex. One of the key constraints of this battlespace is that only 1 percent of the spectrum accounts for 90 percent of its military and civilian use. The effectiveness of the EMS is also complicated by electromagnetic interference between systems, EMP, competition between military and civilian use, and natural phenomena such as lightning, solar flares, and precipitation. Additionally, it is important to emphasize that our adversaries know and understand the EMS and that they will aggressively contest our access to it. Use of the spectrum requires coordinated, prioritized, and deconflicted operations. Supported joint force commanders hold the authority for assigning frequencies to users, and once frequencies are allocated to systems within a specific geographical area, they are no longer available for use This fact necessitates that commanders and their staffs understand how to operationally assess the impact of forfeiting the use of spectrum-dependent systems in order to employ other capabilities.

The international environment further obscures effective use of the EMS in support of military operations. The spectrum transcends all physical domains, has no specific or internationally recognized boundaries, and can create a wide array of unintended collateral effects ranging from the annoyance of a communication disruption to a deadly collision on a civilian railway transit system. Accordingly, approval to use electromagnetic-dependent systems for military operations calls for extensive coordination with multinational allies and host nations. It also mandates an innovative level of operational planning that facilitates prioritized allocation of bandwidth, efficient data exchange, flexible security requirements, and the organizational processes necessary to support the operation.

How Does This Change in Operational Environment Affect Airpower?

The dramatic alterations now occurring across the operational environment will affect airpower in innumerable ways, including air superiority, strategic attack, counterland, countermaritime, and support to special operations forces. However, the two most significant effects will involve planning, decision, and execution cycles and domain superiority. In the future, these cycles will be compressed, reachback capabilities will be limited, and forward commanders will have to rely on mission-type orders because the EMS will be vigorously contested and because both terrestrial and space-based communications will suffer degradation or disruption. Consequently, airpower's foundational principle of centralized control / decentralized execution will be forced to shift to a distributed-control approach that adapts to operational changes by having preplanned bandwidth allocations and a vision for maneuvering between gateways.

The impending operational environment will also influence the concept of domain superiority. As advanced technology continues to proliferate, domain superiority will be much harder to achieve. In fact, such superiority will most likely remain localized and temporary. Moreover, it is important to point out that success may not depend upon the traditional quest for domain superiority. Instead, success may reside in precision access in a single domain that enables a combination of actions in other domains. Airmen must become much more attuned to forms of maneuver in all of these realms, and until they develop an appreciation for and understanding of multidomain maneuver, true innovation in airpower, unfortunately, will be lacking.

Conclusion

When General Dempsey asked, "What's after joint?" he was emphasizing that at some point in time, the focus on joint operations will not be adequate to address the challenges of our emerging operational environment. During the past two decades, airpower has given the joint force unrivaled dominance in the air. However, quantum advances in technology and the realities of fiscal constraints are driving a dynamic era of evolutionary adaptation. This evolution must be deliberately shaped to ensure that domain interdependence does not inadvertently risk a single point of failure. More than ever before, Airmen must have a clear and common understanding of simultaneous maneuver in multiple domains beyond air, space, and cyberspace. ✪

Notes

1. The Military Education Coordination Council serves as an advisory body to the director of the Joint Staff on joint education issues. The council's principals are the Deputy J-7, the Deputy Director Joint Staff-Military Education; the presidents, commandants, and directors of the joint and service universities and colleges; and the heads of any other institutions accredited by joint professional military education.

2. Currently, no doctrinal definition of *domain* exists. This analysis defines the term as a critical sphere of operational influence whose control provides the foundation for freedom of action. Cross-domain operations involve the exploitation of asymmetric advantage across multiple domains to achieve the freedom of action required by the mission.

3. Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (19 April 1965): 114–17.

4. John Markoff, "IBM Discloses Working Version of a Much Higher Capacity Chip," *New York Times*, 9 July 2015, http://www.nytimes.com/2015/07/09/technology/ibm-announces-computer-chips-more-powerful-than-any-in-existence.html?_r=0,9.

5. Ibid.

6. Mark Gunzinger with Chris Dougherty, *Changing the Game: The Promise of Directed-Energy Weapons* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), ix.

7. Department of Defense, *Joint Operational Access Concept*, version 1.0 (Washington, DC: Department of Defense, 2012), 16.

8. Thucydides, *History of the Peloponnesian War*, trans. Rex Warner (New York: Penguin Books, 1954).

9. Department of Defense, *Joint Operational Access Concept*, 15.

10. Office of the US Air Force Chief Scientist, *Technology Horizons: A Vision for Air Force Science and Technology, 2010–2030* (Maxwell AFB, AL: Air University Press, Air Force Research Institute, 2011), 19.

11. Amy Chang, *Indigenous Weapons Development in China's Military Modernization*, US-China Economic and Security Review Commission Staff Research Report (Washington, DC: US-China Economic and Security Review Commission, 5 April 2012), 21.

12. National Air and Space Intelligence Center, *Ballistic and Cruise Missile Threat*, NASIC-1031-0985-09 (Wright Patterson AFB, OH: National Air and Space Intelligence Center, April 2009), 3.

13. Victor N. Corpus, "America's Acupuncture Points, Part 2: The Assassin's Mace," *Asia Times*, 20 October 2006, http://www.atimes.com/atimes/China/HJ20Ad01.html.

14. National Air and Space Intelligence Center, *Ballistic and Cruise Missile Threat*, 27.

15. US General Accounting Office, *Nonproliferation: Improvements to Better Control Technology Exports for Cruise Missiles and Unmanned Aerial Vehicles*, GAO-04-175 (Washington, DC: US General Accounting Office, January 2004), 6.

16. US Government Accountability Office, *Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports*, GAO-12-536 (Washington, DC: US Government Accountability Office, July 2012), 9.

17. National Ground Intelligence Center, *China Research on Bio-Effects of Electromagnetic Pulse and High-Power Microwave Radiation* (Charlottesville, VA: National Ground Intelligence Center, 17 August 2005). Unclassified.

18. Headquarters Department of the US Army, *Nuclear Environment Survivability* (US Army White Sands Missile Range, NM: US Army Test and Evaluation Command, 15 April 1994), appendix D.

19. See Chuck Hansen, *U.S. Nuclear Weapons: The Secret History* (Arlington, TX: Aerofax, 1988), 78–79 and 81.

20. See Jim Wilson, "E-Bombs and Terrorists," *Popular Mechanics* 178*,* no. 9 (September 2001): 51; and Frederic P. Miller, Agnes F. Vandome, and John McBrewster, *Explosively Pumped Flux Compression Generator* (Mauritius: Alphascript Publishing, 24 November 2009).

21. Department of Defense, *Joint Operational Access Concept*, 13.

22. Andrew F. Krepinevich, *7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century* (New York: Bantam Dell, 2009), 187.

23. John E. Bruzdzinski, "Demystifying Sha Shou Jian: China's 'Assassin's Mace' Concept," in *Civil-Military Change in China: Elites, Institutes, and Ideas after the 16th Party Congress*, ed. Andrew Scobell and Larry Wortzel (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, December 2005), 345.

24. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 145–46.

25. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* [Milpitas, CA: Mandiant, n.d.], accessed 4 December 2015, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

26. Deepak Sharma, "China's Cyber Warfare Capability and India's Concerns," *Journal of Defence Studies* 5, no. 2 (April 2011): 66.

27. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2013* (Washington, DC: Office of the Secretary of Defense, 2013), 36.

28. Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare," *Journal of Defence Studies* 4, no 2 (April 2010): 37–38.

29. Bruzdzinski, "Demystifying Sha Shou Jian," 346.

30. Office of the Secretary of Defense, *People's Republic of China, 2013*, 37.

31. Gunzinger with Dougherty, *Changing the Game*, 5.

32. United States Government Accountability Office, *Information Security: Weaknesses Continue amid New Federal Efforts to Implement Requirements*, GAO-12-137 (Washington, DC: United States Government Accountability Office, October 2011), 4.

33. Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 4.

34. House of Representatives, *Electric Grid Vulnerability: Industry Responses Reveal Security Gaps*, report written by the staff of Congressman Edward J. Markey (D-MA) and Henry A. Waxman (D-CA)

(Washington, DC: House of Representatives, 21 May 2013), 12, https://portal.mmowgli.nps.edu/c/document_library/get_file?uuid=b2f47e65-330e-4d89-adee-e2ed58908927&groupId=10156.

35. See US-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (Washington, DC, and Ottawa: US-Canada Power System Outage Task Force, April 2004), 17–18; and JR Minkel, "The 2003 Northeast Blackout—Five Years Later," *Scientific American*, 13 August 2008, http://www.scientificamerican.com/article/2003-blackout-five-years-later/.

36. Brenner, *America the Vulnerable*, 110.

37. David Wright, Laura Grego, and Lisbeth Gronlund, *The Physics of Space Security: A Reference Manual* (Cambridge, MA: American Academy of Arts and Sciences, 2005), 109.

38. Shirley Kan, *China's Anti-satellite Weapon Test*, CRS Report for Congress (Washington, DC: Congressional Research Service, 23 April 2007), 1.

39. Craig Murray, *China Missile Launch May Have Tested Part of a New Anti-satellite Capability*, Staff Research Backgrounder (Washington, DC: US-China Economic and Security Review Commission, 22 May 2013), 2.

40. Joint Publication 3-14, *Space Operations*, 29 May 2013, I-9, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

41. Joint Publication 6-01, *Joint Electromagnetic Spectrum Management Operations*, 20 March 2012, I-1, http://www.dtic.mil/doctrine/new_pubs/jp6_01.pdf.

42. United States Government Accountability Office, *Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight*, GAO-12-479 (Washington, DC: United States Government Accountability Office, July 2012), 1.

43. United States Government Accountability Office, *Airborne Electronic Attack: Achieving Mission Objectives Depends on Overcoming Acquisition Challenges*, GAO-12-175 (Washington, DC: United States Government Accountability Office, March 2012).

Dr. Jeffrey M. Reilly

Dr. Reilly (MA, University of Houston; PhD, University of Alabama), a retired Army officer with 26 years of active duty service, has held numerous command and staff positions as an infantry officer. His planning and operations experience includes serving as a theater-level combined and joint operations officer, plans division chief, and member of the "two major theater war" plans team. He has been an adjunct faculty member for the NATO School's Comprehensive Operational Planning Course, a frequent speaker at the USAF Weapons Instructor Course, and a member of the chairman of the Joint Chiefs of Staff's Military Education Coordination Council Working Group. Dr. Reilly has also given a number of presentations at international defense colleges, including the Führungsakademie der Bundeswehr, in Hamburg, Germany; the Ethiopian Defense Staff College in Addis Ababa; and the Polish National Defense University in Warsaw. Additionally, he conducted research on design in Afghanistan during 2010, 2011, and 2012. The author of *Operational Design: Distilling Clarity from Complexity for Decisive Action* (Air University Press, 2012), Dr. Reilly currently serves as director of joint education at the Air Command and Staff College and as director of the college's Multi Domain Operational Strategist concentration.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

http://www.airpower.au.af.mil