

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

**DISTINCTIVE FUNCTIONS OF THE UNITED STATES AIR FORCE IN THE
CYBERSPACE DOMAIN**

By

Andrew K. Hosler, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lt Col Paul Griffith

Maxwell Air Force Base, Alabama

December 2009

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

Cyberspace is a domain shared by all military services and is critical to integrating forces in the joint warfight. As the subunified command develops under USSTRATCOM, the services must assess their particular potential and capabilities within the cyberspace domain. This paper seeks to define the Air Force niche within cyberspace. It proposes a perspective that the distinctive capabilities of the Air Force within its physical domains inherently make it the service to appropriate lead in three distinctive functions: operational reachback to a fixed base, parallel attack, and preparation of the battlespace. A research review built upon the concepts of operating in cyberspace and the tenets of air and space power drive the results.

In today's American warfighting environment, it is clear that cyberspace is not just a domain shared among all services, it is also a domain shared with the world.¹ According to the National Military Strategy for Cyberspace Operations, "operations in cyberspace are a critical aspect of our military operations around the globe."² Cyberspace operations must be integrated into other domains to achieve the greatest effects making it an inherently joint domain.³ Considering the global, ubiquitous nature of the domain and understanding the criticality of properly integrating joint forces, the Department of Defense granted responsibility for developing military capabilities and doctrine within the domain to United States Strategic Command rather than any individual service.⁴ The task to the services then becomes one of presenting forces to the joint combatant command and, more basically, finding the service niche in cyberspace. Per the United States Air Force Blueprint for Cyberspace, the USAF must "develop unique cyber capabilities that originate in its distinct missions and take full advantage of the integration of air, space and cyber capabilities."⁵ In fact, the document identifies this requirement as the first objective to be met in the Air Force's drive towards fully competent cyberspace operations.⁶ The statement echoes the recommendation of recent research while backing off the perspective of earlier theorists who claimed the technological focus of the Air Force made it the natural choice to lead the military into the cyber domain.⁷ In fact, any service may adapt technology to improve its capabilities; the proof is evident in every major weapons systems purchase and upgrade. The analogy to the air domain is apt here. While all services retain a capability to function in the air, their air components support their respective traditional domain missions. The Air Force alone makes the air and space domains their primary domains of warfare and has structured itself appropriately to support air and space missions. Similarly, the cyberspace domain is a shared domain necessary to support the network-centric warfare

adopted by each of the services. However, the characteristics that make the Air Force capable and distinguishable in its physical air and space domains also lead the Air Force to distinguish itself among the services with distinctive functions in the cyberspace domain. These distinctive functions include operational reachback to a fixed base, parallel attack, and preparation of the battlespace.

“Cyberspace,” as defined by the National Military Strategy for Cyberspace Operations, is “a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”⁸ By its nature, cyberspace is a domain that rewards technical innovation, control of volatility, and speed.⁹ While the Department of Defense transformation initiative seeks to modernize warfighting capabilities via a concept of network-centric operations expecting that technology will drive new doctrine, services cannot ignore the truths of fighting in their respective domains. In Air Force doctrine these truths are referred to as tenets of air and space power, shown in Table 1 of the Appendix.¹⁰ Woolley wrote that all tenets of air and space power also apply to cyber with the addition of three others that are distinct to the cyberspace domain: responsiveness, reliability, and global perspective.¹¹ These air and space power tenets, as well as familiarity with analogs of the distinctly cyberspace tenets within the physical domain, are precisely the features of the Air Force that allow it to be a relevant force for specific military functions of cyberspace. For instance, the speed and maneuver of air power compared to forces fighting in other physical domains is somewhat analogous to the responsiveness tenet of cyberspace. Similarly, reliability may be analogous to the persistent presence of air and space dominance over a battlefield, and global presence may be analogous to the inherent global reach of air and space power.

Convertino, DeMattei, and Knierim wrote that military cyberspace operations should seek to achieve three goals: provide intelligence related to enemy networks, provide assurance of friendly networks, and provide the ability to “influence, engage, and prevail against the enemy.”¹² Table 2 (see Appendix) matches these three stated goals with proposed cyberspace distinctive functions of the Air Force: preparation of the battlespace, operational reachback to a fixed base, and parallel attack. The table also presents tenets of air and space power that pertain to the proposed distinctive functions and further gives an example of how the functions are relevant and practiced in the physical domains. A discussion of each distinctive function follows.

Operational reachback to a fixed base refers to the ability to access friendly remote systems with faith in system integrity and confidentiality.¹³ System integrity and confidentiality speak to the reliability tenet of cyberspace.¹⁴ DoDD 5100.1, which defines the functions of each of the services, gives responsibility for air and space imagery and air and space lines of communication to the Air Force sealing its capability and requirement to provide a reachback role in cyberspace.¹⁵ This distinctive function relies on persistent links back to a secure site and utilizes both the inherent reachback and global situational awareness capabilities of space and those communication links provided by forward deployed aircraft.¹⁶ Airmen must operate bases to support aerial missions in the physical domain and are, therefore, always tied to a specific piece of land regardless of their actual location.¹⁷ Just as a commander actively defends his base to enable aircraft to return and “preserve the ability to wage war”, so too must the Air Force defend its core information systems to enable confident reachback in cyberspace.¹⁸ This is accomplished, just as in the physical domain, with persistent, flexible, and versatile active and

passive defenses. Flexibility and versatility in airpower with global reach provides excellent options for a commander to defend and reconstitute, if necessary.¹⁹

Parallel attack refers to the ability to strike enemy interests at any geographic location at the tactical, operational, and strategic levels simultaneously.²⁰ This distinctive function truly lies at the heart of the Air Force mission encompassing all tenets of air and space power. It is derived from the speed and maneuver displayed by Air Force weapon systems able to strike with “timely concentration, employment, and sustainment of United States military power anywhere – at our initiative, speed, and tempo.”²¹ This includes traditional Air Force strike missions such as strategic attack, counterair, counterland, counterspace, close air support, and interdiction.²² Just as important as speed and maneuver, this specialty relies on “precision engagement” to achieve effects, a distinctive capability of the Air Force as “the Service with the greatest capacity to apply the technology and techniques of precision engagement anywhere on the face of the Earth in a matter of hours.”²³

Preparation of the battlespace refers to the ability to persist in and exploit an adversary’s network to gain intelligence or in preparation for an offensive or defensive action.²⁴ This distinctive function ties directly to Convertino, DeMattei, and Kneirim’s goal of providing intelligence of the enemy network.²⁵ The Air Force’s space mission inherently requires a persistent, global perspective.²⁶ Its airborne sensors provide near real-time reconnaissance and persistent surveillance in support of operations worldwide. Timeliness, persistent presence, and a global perspective are also inherent in cyberspace operations.²⁷ In air and space, the Air Force provides a “high ground” that the joint U.S. military may exploit.²⁸ Cyberspace offers the joint warfighter the next “high ground” and, by some accounts, the first that must be exploited in

preparation for successful operations.²⁹ The inherent relationship among air, space, and cyberspace points to the Air Force as a provider of this distinct cyberspace function.

As observed by Hare and Zimmermann, in the joint fight today “we cannot achieve victory without dominating across all three domains: air, space and cyberspace.”³⁰ Just as today’s American warfighter expects air and space freedom of action, they also depend on cyberspace dominance.³¹ Though cyberspace offers new limits to warfare principles such as speed and maneuver, the Air Force is used to fighting near the physical limits of these principles. All services must integrate their capabilities within the cyberspace domain, however, the nature of the Air Force and air and space power support specific niche functions for the Air Force within the domain. For more reasons than simply claiming its rights as the “technocratic” service, the Air Force has a requirement to present cyber forces to the combatant commander as specialists in three areas: preparation of the battlespace, operational reachback to fixed bases, and parallel attack. The tenets of air and space power meld with these cyber specialties and will support the Air Force in being leaders among the services in these functions. As directed by the first step of the USAF Blueprint for Cyberspace, the Air Force must recognize these niche functions in this newest of warfighting domains and exploit them to their fullest potential in order to support the joint warfighter.³²

¹ Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 15

² US Department of Defense, *National Military Strategy for Cyberspace*, vii.

³ Alexander, “Warfighting in Cyberspace”, 60.

⁴ Ibid., 60.

⁵ Air Force Space Command, *USAF Blueprint for Cyberspace*, 6.

⁶ Ibid., 9.

⁷ Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 33; Szafranski and Libicki, “...Or Go Down in Flame”, 2. Convertino, DeMattei, and Kneirim recognized that, as a member of a joint force, the Air Force must define its niche in cyberspace rather than rally for full control. Szafranski and Libicki argued that the same drive leading airmen to implement the technology of the airplane in the aerial domain is inherent in the Air Force and, thus,

should lead the Air Force to take a military interest and lead in cyberspace. Later in their paper, they argued that also the inherent connection among air, space, and cyberspace should drive the Air Force to lead in the cyberspace domain above the other services.

⁸ US Department of Defense, *National Military Strategy for Cyberspace*, ix.

⁹ US Department of Defense, *National Military Strategy for Cyberspace*, 4.

¹⁰ AFDD-1, *Air Force Basic Doctrine*, 27-33. Definitions for each of the tenets of air and space power are partially directly quoted from the AFDD and partially paraphrased where the author felt it was appropriate for clarification of the concept.

¹¹ Woolley, "Defining Cyberspace", 40-42.

¹² Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 12-13.

¹³ Libicki, *Cyberwar and Cyberdeterrence*, 162.

¹⁴ Woolley, "Defining Cyberspace", 42.

¹⁵ DODD 5100.1, *Functions of the Department of Defense*, 21-23.

¹⁶ Air Force Space Command, *USAF Blueprint for Cyberspace*, 4.

¹⁷ Grant, *Victory in Cyberspace*, 23.

¹⁸ Libicki, *Cyberwar and Cyberdeterrence*, 162; Courville, "Air Force and the Cyberspace Mission Defending," 25.

¹⁹ Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 50. Reconstitution is presented as a key component of cyber defense.

²⁰ US Department of Defense, *Implementation of Network-Centric Warfare*, 55.

²¹ AFDD 1, *Air Force Basic Doctrine*, 48. This entry includes a definition derived from that of agile combat support, a capability reliant on global reach.

²² AFDD 2-5, *Information Operations*, 14, 29.

²³ AFDD 1, *Air Force Basic Doctrine*, 80; Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 42.

²⁴ AFDD 2-5, *Information Operations*, 21-23.

²⁵ Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 12-13.

²⁶ Brooks, et al., "Presentation of Cyber Forces", 27-28.

²⁷ Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 41, 47; AFDD 2-11, *Cyberspace Operations*, 38.

²⁸ Szafranski and Libicki, "...Or Go Down in Flame", 2.

²⁹ Szafranski and Libicki, "...Or Go Down in Flame", 2, 5; Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 58. Convertino, DeMattei, and Kneirim presented an argument that a cost / benefit analysis favors a cyberspace attack and exploitation above operations conducted in physical domains.

³⁰ Hare and Zimmermann, "The Air Force in Cyberspace", 94.

³¹ Rogers, "Shaping the Air Force", 11; Radice, "Dominating Cyberspace", 2. Both authors relate a concept of dominance in the cyberspace domain by joint forces.

³² Air Force Space Command, *USAF Blueprint for Cyberspace*, 9.

Appendix

Tenets of Air / Space	Explanation
Centralized control / decentralized execution	Planning, direction, prioritization, synchronization, integration, and deconfliction of air and space capabilities to achieve the objectives of the joint force commander The delegation of execution authority to responsible and capable lower-level commanders to achieve effective span of control and to foster disciplined initiative, situational responsiveness, and tactical flexibility
Flexibility and versatility	Ability to exploit mass and maneuver simultaneously; to shift from one campaign to another Ability to employ air and space power effectively at the strategic, operational, and tactical levels of warfare
Synergistic effects	The proper application of coordinated force to produce effects that exceed the contributions of forces employed individually
Persistence	Ability to conduct operations continuously against a broad spectrum of targets
Concentration	Ability and versatility to mass forces with overwhelming power at the right time and right place
Priority	Ability to assess possible uses of limited available force and apply them where they can make the greatest contribution to the most critical joint force commander requirements
Balance	Ability to balance combat opportunity, necessity, effectiveness, efficiency, and impact on accomplishing assigned objectives against the associated risk to friendly air and space forces

Table 1. The Tenets of Air and Space Power. Source AFDD 1, Air Force Basic Doctrine.

Convertino, DeMattei, and Knierim Goals	Proposed Distinctive Functions	Explanation	Supporting Tenets	Physical Example
Know the adversary networks	Preparation of battlespace	Ability to persist in and exploit an adversary's network to gain intelligence or in preparation for an offensive or defensive action	Persistence Flexibility and versatility Priority Balance	Air and space dominance allows persistent loitering of ISR assets over enemy territory
Assurance of systems and ability to operate in and shape the cyberspace environment	Operational reachback to fixed base	Ability to access friendly remote systems with trust in system integrity and confidentiality* Libicki	Persistence Flexibility and versatility Balance Priority	Air base provides fixed secure location for aircraft to return / coordinate actions
Military operational advantage in cyberspace to influence, engage, and prevail against the enemy	Parallel attack	Ability to strike enemy interests at any geographic location at the tactical, operational, and strategic levels simultaneously	Persistence Flexibility and versatility Synergistic effects Centralized control / decentralized execution Concentration Priority Balance	Air power provides capability to strike deep behind enemy lines and attack tactical, operational, or strategic targets

Table 2. Proposed Air Force Distinctive Functions in the Cyberspace Domain and Supporting Air and Space Tenets

Bibliography

- Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine*. 17 November 2003.
- Air Force Doctrine Document (AFDD) 2-5. *Information Operations*, 5 August 1998.
- Air Force Doctrine Document (AFDD) 2-11 (DRAFT Document). *Cyberspace Operations*, Draft acquired from Curtis E. LeMay Center for Doctrine Development and Education, Maxwell Air Force Base, AL. Tentatively dated 2008.
- Air Force Space Command Headquarters Staff. "The United States Air Force Blueprint for Cyberspace." Peterson Air Force Base, CO. 2 November 2009.
- Alexander, LT GEN Keith B. "Warfighting in Cyberspace." *Joint Forces Quarterly*, Issue 46 (3rd Quarter 2007), 58-61.
- Brooks, Col Todd A., Col Anthony J. Zucco, Lt Col L. Dean Worley, Jr., Lt Col James A. Davis. "Presentation of AFCyber Forces: A Hybrid Approach." Maxwell Air Force Base, AL: Air University, Air War College, 24 February 2008.
- Convertino, Lt Col Sebastian M., II, Lou Anne DeMattei, and Lt Col Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Maxwell Air Force Base, AL: Air University Press, 2007.
- Courville, Lt Col Shane P. "Air Force and the Cyberspace Mission Defending the Air Force's Computer Network in the Future." Maxwell Air Force Base, AL: Air University, Air War College, Center for Strategy and Technology, December 2007.
- Department of Defense (DOD) Directive 5100.1. *Functions of the Department of Defense and Its Major Components*, 1 August 2002.
- Grant, Rebecca. *Victory in Cyberspace*. Arlington, VA: Air Force Association, October 2007.
- Hare, Forrest B. and Glenn Zimmerman. "The Air Force in Cyberspace: Five Myths of Cyberspace Superiority." In *Military Perspectives on Cyberpower*, edited by Larry K. Wentz, Charles L. Barry, and Stuart H. Starr, 87-95. Washington, D.C.: National Defense University, Center for Technology and National Security Policy, July 2009.
- Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA, Arlington, VA, Pittsburgh, PA: RAND Corporation, 2009.
- Radice, Cmdr Richard A. "Dominating Cyberspace." Carlisle Barracks, PA: US Army War College, 12 March 2007.
- Rogers, John C. "Shaping the Air Force Operational Environment in Cyberspace." Maxwell Air Force Base, AL: Air University, Air War College, 12 February 2009.

Szafranski, Col Richard and Dr. Martin Libicki. “’...Or Go Down in Flame’? An Airpower Manifesto for the 21st Century.” In *2025*. Maxwell Air Force Base, AL: Air University Press, August 2006. Published online at <http://csat.au.af.mil/2025/index.htm>, accessed 1 December 2009.

US Department of Defense. *The Implementation of Network-Centric Warfare*. Washington, D.C.: Office of the Secretary of Defense (Force Transformation), 5 January 2005.

US Department of Defense. *The National Military Strategy for Cyberspace Operations (U)*. Washington, D.C.: Chairman of the Joint Chiefs of Staff, December 2006.

Woolley, Maj Pamela L. “Defining Cyberspace as a United States Air Force Mission.” Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, June 2006.