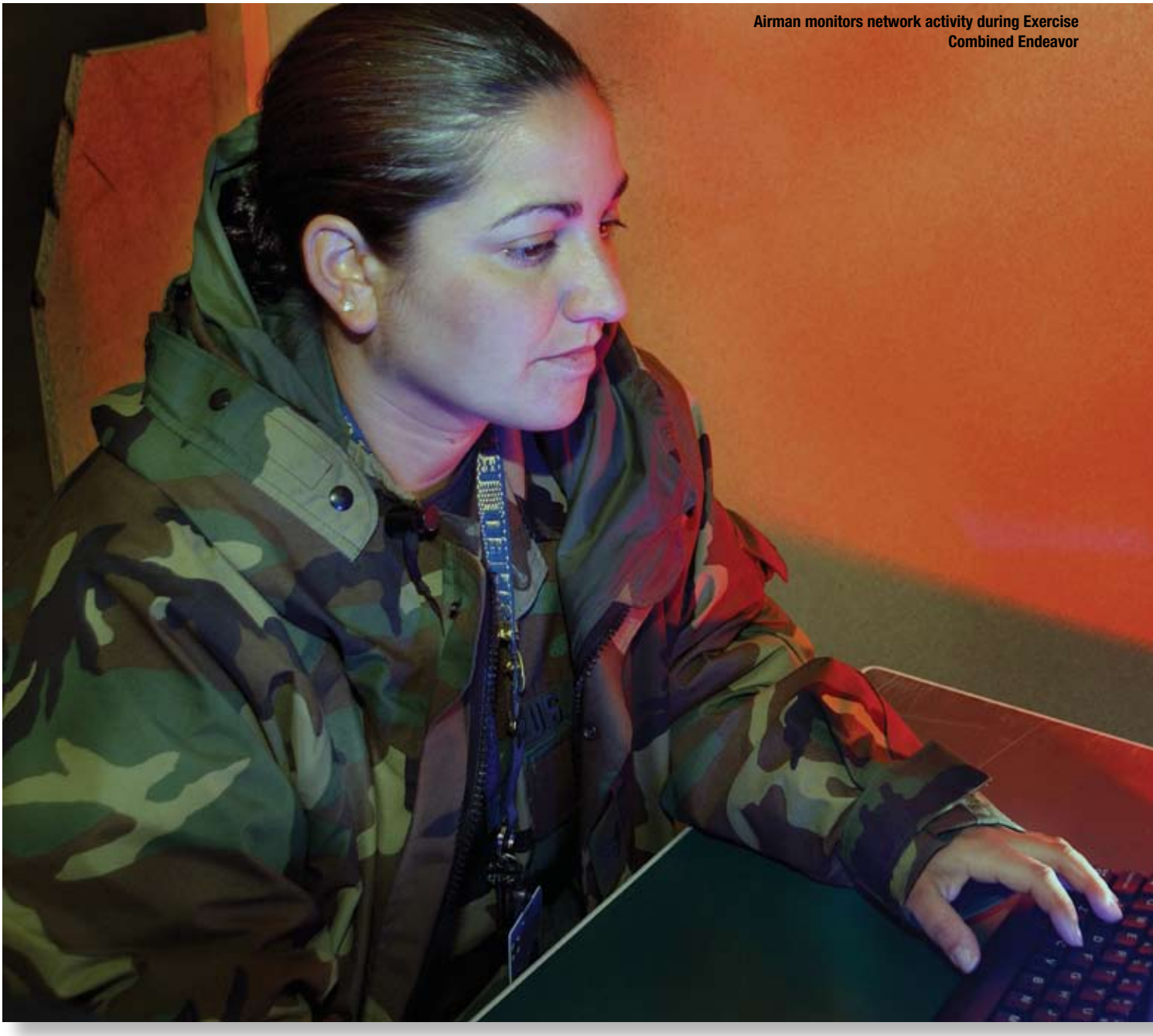
# Warfighting in Cyberspace

*By* KEITH B. ALEXANDER



Airman monitors network activity during Exercise Combined Endeavor

Lieutenant General Keith B. Alexander, USA, is Director, National Security Agency, and Commander, Joint Functional Component Command for Network Warfare.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2007** | | **00-00-2007 to 00-00-2007** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Warfighting in Cyberspace** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies,260 Fifth Avenue SW Bg 64 Fort Lesley J. McNair,Washington,DC,20319** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **4** | |

Secretary of the Air Force, Michael W. Wynne, discusses creation of Cyberspace Command

U.S. Air Force (Cohen Young)

U.S. Air Force (Thomas Meneguin)

Our current and potential adversaries clearly understand the military potential of cyberspace and the expansive power of the medium. Terrorists employ the Internet for recruiting, training, motivating, and synchronizing their followers. They can operate essentially unrestrained and are free to innovate, unbound by law, policy, or precedent. Nations such as China and Russia are developing their own "cyberspace warriors." China, for instance, has formed cyberspace battalions and regiments, the primary purpose of which is to identify and exploit weaknesses in our military, government, and commercial networks.[1] In November 1999, the *PLA Daily* stated, "Internet warfare is of equal significance to land, sea, and air power and requires its own military branch," and that "it is essential to have an all-conquering offensive technology and to develop software and technology for net offensives . . . able to launch attacks and countermeasures."

The threat from these forces is credible and real. While the time-tested principles of war will ultimately apply in cyberspace, its characteristics are so radically different that they demand significant innovation and changes to the way we organize and conduct military operations and tactics in this domain.

Many within the U.S. Government and private sector are beginning to recognize the importance of cyberspace (and operations within it) to national security. The March 2005 National Defense Strategy identified cyberspace as a new theater of operations and assessed cyberspace operations as a potentially disruptive challenge, concluding that in "rare instances, revolutionary technology and associated military innovation can fundamentally alter long-established concepts of warfare."[2] The Chairman of the Joint Chiefs of Staff concluded in the 2004 National Military Strategy:

*The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace. Armed Forces must employ military capabilities to ensure access to these domains to protect the nation, forces in the field and U.S. global interests. . . . Along with technological solutions to improve joint war fighting, we must also examine our doctrine, organization, training, materiel, leadership and education, personnel and facilities to ensure military superiority.*[3]

Despite this emphasis, however, we can argue that, while we have ample national level strategies, we have yet to translate these strategies into operational art through development of joint doctrine for cyberspace. Through the doctrine vetting process, we can develop a common understanding of what it means to conduct warfare within and through cyberspace. The ultimate strategic objective of these operations is to ensure U.S. freedom of action in cyberspace and to deny the enemy the same.

Development of cyberspace doctrine is a complex task; the only doctrine that currently addresses operations within the cyberspace environment is contained within two subsets of information operations (IO): computer network operations and electronic warfare (EW). Since computer network operations and EW are exclusively conducted through "the use of electronics and the electromagnetic spectrum," there is an overlap between IO activities and what our national strategy defines as military capabilities in the cyberspace domain (that is, cyber warfare). Although the defensive elements of IO and cyber warfare are important, to narrow the scope of our thesis, the remainder of the argument will principally focus on the offensive elements.

*through the doctrine vetting process, we can develop a common understanding of what it means to conduct warfare within and through cyberspace*

Joint Publication (JP) 3–13, *Information Operations*, defines *IO* as "the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking while protecting our own."[4] JP 3–13 also states "for the purpose of military operations, computer network operations are divided into computer network attack, computer network defense, and related computer network exploitation enabling operations."

## Cyberspace as a Warfighting Domain

The common theme that runs through IO doctrine is its focus on affecting the human or automated cognitive or intellectual processing of information. JP 3–13 states, "The focus of IO is on the decisionmaker and the information environment in order to affect decisionmaking and thinking processes, knowledge, and understanding of the situation." Since the "ultimate strategic objective" of IO is "to deter a potential or actual adversary . . . from taking actions that threaten U.S. national interests," then to be successful, IO must encompass all actions taken by the U.S. Government. Even though the recent revision of JP 3–13 narrows IO doctrine to "five core capabilities," it still seeks to employ other "supporting and related capabilities" that in effect encompass nearly all Government actions.[5] Under IO doctrine, any statement we make, any movement of U.S. forces, or any bomb we drop could be considered a form of fires in an information operation if its principal intent is to influence adversary decisions away from taking action against our will.

Now, let us contrast IO doctrine with what we propose for cyber warfare. The focus of cyber warfare is on using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability, while protecting our own. Instruments unique to cyber warfare are narrowly confined to those activities described in the definition: EW and computer network operations. When we conduct any military operation, we must integrate and synchronize all available instruments of warfare in all domains. It is clearly understood that land, maritime, air, and space warfare are, in and of themselves, important warfighting activities that ensure the U.S. military's ability to maintain freedom of action while denying an adversary the same. Although it is understood that land, maritime, air, and space warfare will be employed to deter (for example, influence) an adversary, no one believes that warfare within these domains is uniquely "information operations." Where the principal effect of IO is to influence an adversary *not* to take an action, the principal effect of cyber warfare is to deny the enemy freedom of action in cyberspace. Granted, by denying enemies' freedom of action in cyberspace, we will also influence them; however, influence is not the intended primary effect—denying freedom of action is the intended primary effect.

Airmen monitor Internet traffic

U.S. Air Force (Jack Braden)

It may seem that we are arguing to remove EW and computer network operations from IO doctrine. We are not. What we are arguing for is that just as we have now come to recognize cyberspace as a new warfighting domain, so too must we recognize that it is equal to the other warfighting domains and doctrine should reflect such. Now is the time to update our doctrine to establish fundamental cyber warfare principles that guide employment of EW and computer network operations forces in support of our national objectives.

## Operationalizing Cyberspace Warfare

U.S. Strategic Command (USSTRATCOM) has already begun to implement this shift. The commander, beginning in Unified Command Plan (UCP) 2002 and carried forth in subsequent UCPs, was given the responsibility for "integrating and coordinating [Department of Defense] IO that cross geographic areas of responsibility or across the core IO capabilities, including identifying desired characteristics and capabilities for computer network attack and conducting computer network attack in support of other combatant commanders, as directed."[6] USSTRATCOM is moving to shift operational focus from the cognitive effects, described

*the principal effect of cyber warfare is to deny the enemy freedom of action in cyberspace*

within IO, to a common planning framework for the Defense Department to achieve specific cyberspace objectives. We have redefined our cyberspace mission area in terms of offensive–network warfare (NW) and defensive–network operations (NetOps)—and established JFCC–NW and JTF–GNO to address each of those mission sets, respectively.

As directed by the USSTRATCOM commander, the Joint Functional Component Command for Network Warfare (JFCC–NW) was established to "optimize planning, execution, and force management for the assigned missions of deterring attacks against the United States, its territories, possessions, and bases, and employing appropriate forces should deterrence fail, and the associated mission of integrating and coordinating [Defense Department] CNA [computer network attack] and computer network defense as directed by headquarters USSTRATCOM."[7] The command further defines *network warfare* as "the employment of computer network operations with the intent of denying adversaries the effective use of their own computers, information systems, and networks."[8] This mission statement recognizes the primacy of the strike or attack aspects of computer network attacks as a military fire, not merely as an enabler for cognitive effects.

USSTRATCOM has also begun to develop tactics, techniques, and procedures and other concepts designed to integrate cyberspace capabilities into cross-mission strike plans. We are developing concepts to address warfighting in cyberspace in order to assure freedom of action in cyberspace for the United States and our allies while denying adversaries and providing cyberspace-enabled effects to support operations in other domains.[9] These concepts, and the cyberspace effects that they focus on, are clearly based on the military concepts of strike, fires (supporting and suppressing), and defense.

While the concepts of NW and NetOps are a good start, they represent only a small subset of the elements of military power available within or enabled by cyberspace. In order to fully engage in the development of joint doctrine within the cyberspace domain, it is also necessary to develop a definition of exactly what warfare within cyberspace—or cyberspace warfare—is.

JP–1 describes a joint doctrine development process that starts with a project proposal and then moves through a program directive, developing and staffing drafts prior to receiving approval from the Chairman of the Joint Chiefs of Staff. We need to engage this process to codify the planning, operational, and support systems required to execute this rapidly emerging form of warfare that focuses on how we will plan and execute operations within the arena. Our challenge is establishing recognizable doctrine that will include definitions and fundamental principles to guide the employment of military forces and weapon systems for operations within the cyberspace domain.

In coming to grips with military operations in cyberspace, we face many challenges that are strikingly similar to what our military faced during the Interwar Years from 1919 to 1938. During this period, the military struggled with mechanization and the revolution in military affairs that it fostered. Airpower in particular came into its own, but not without great frustration and sacrifice on the part of visionary airpower advocates. Despite significant advances in air combat during World War I, the Army, which controlled most U.S. airpower, was hesitant to move forward. Only after nearly 20 years of struggle and the high-profile court martial of Billy Mitchell were airpower advocates able to make the advances in operations, tactics, and materiel in the air domain that proved crucial to the Allied victory in World War II.

The speed at which the cyberspace domain is evolving and its ever-growing impact on national security make this potentially as critical a period as that faced by Mitchell, Claire Chennault, and their contemporaries as they realized the potential of the air domain and sought to develop airpower doctrine. Unfortunately, we do not have the luxury of 20 years to develop strategy, tactics, and doctrine to deal with this revolution and maintain U.S. superiority in this rapidly changing environment. The trends for advances in technology, often (correctly or incorrectly) related to Moore's Law and derivative theories, such as the Law of Accelerating Returns proposed by Ray Kurzweil in his 2001 essay, dictate that we must move quickly.[10] If one examines the advances in Internet and computer technology in just the last 5 years, it is readily apparent that we could find ourselves behind or even militarily irrelevant in cyberspace.

*USSTRATCOM has also begun to develop tactics, techniques, and procedures and other concepts designed to integrate cyberspace capabilities into cross-mission strike plans*

It is imperative that we capture the lessons learned associated with previous revolutions in military affairs and move quickly and decisively. We must make a dedicated joint effort to develop the forces that will fight and defend our national interests in cyberspace, and we must diligently develop the training and doctrine that will guide them as they execute their critical missions in this new military domain. **JFQ**

## NOTES

[1] Timothy L. Thomas, *Dragon Bytes, Chinese Information War Theory and Practice* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 52–74.

[2] *The National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, March 2005), 4.

[3] *The National Military Strategy of the United States of America* (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, 2004), 18, 23.

[4] Joint Publication 3–13, *Information Operations*, February 13, 2006, available at <www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>.

[5] Recent changes were driven less by operational need to adjust doctrine than by bureaucratic politics. It was principally an effort by individual communities of interest to maintain their hegemony over their domains and not be absorbed into the burgeoning "information operations" bureaucracy. Hence, their new definition of "five core capabilities" and other "supporting and related activities."

[6] Unified Command Plan 2004, March 1, 2005.

[7] JFCC–NW Implementation Directive, January 20, 2005.

[8] Ibid.

[9] USSTRATCOM Brief, January 11, 2007.

[10] Ray Kurzweil, "Law of Accelerating Returns," 2001, available at <http://lifeboat.com/ex/law.of.accelerating.returns>.