Air University
Stephen R. Lorenz, Lt Gen, Commander

Air War College
Stephen J. Miller, Maj Gen, Commandant
Stephen Wright, Col, PhD, Dean
Lawrence E. Grinter, PhD, Series Editor
Stephen Wright, Col, PhD, Essay Advisor

Air University Press
Shirley B. Laseter, DPA, Director
Bessie E. Varner, Deputy Director
Marvin Bassett, PhD, Content Editor
Lula Barnes, Copy Editor
Mary P. Ferguson, Prepress Production
Daniel Armstrong, Cover Design
Bessie E. Varner, Quality Review

Please send inquiries or comments to
Editor
The Maxwell Papers
Air War College
325 Chennault Circle, Bldg. 1401
Maxwell AFB AL 36112-6006
Tel: (334) 953-7074
Fax: (334) 953-1988
http://www.au.af.mil/au/awc/awcgate/awc-mxwl.htm

AIR WAR COLLEGE
AIR UNIVERSITY

Flying and Fighting in Cyberspace

SEBASTIAN M. CONVERTINO II
Lieutenant Colonel, USAF

LOU ANNE DEMATTEI
Defense Intelligence Agency

TAMMY M. KNIERIM
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 40

Air University Press
Maxwell Air Force Base, Alabama

July 2007

Disclaimer

Foreword

On 5 December 2005, the Air Force expanded its mission to include a new domain of war fighting: "to fly and fight in Air, Space, and *Cyberspace*." When the Air Force claimed cyberspace as part of its mission, it not only acknowledged the changing terrain of conflict and a shift in tactics of would-be adversaries but also surprised many in uniform who wondered what the move implied. By changing its mission statement, the Air Force sparked considerable debate on the extent to which cyberspace would dominate roles, missions, and the budget. To organize for this task, the Air Force established a new operational command for cyberspace on 6 September 2006, designating Eighth Air Force as the new Cyber Command.

The Air Force has determined that cyberspace is fundamental to every aspect of war fighting at all levels of operations, and it is seriously engaged in developing cyber capabilities. However, the study's authors argue that the Air Force needs to clearly articulate what Airmen do in cyberspace and how they do it as war fighters. Furthermore, the long lead time to formalize and standardize cyberspace operating concepts and definitions recognizes the complexity and uniqueness of cyberspace as a military operational domain. It also has resulted in a lack of conceptual and doctrinal clarity and consensus on the ends, ways, and means of operating in cyberspace, as well as an unfocused foundation upon which to plan strategy, build and organize forces, and find resources. The study contends that before the Air Force can lead in cyberspace, it must first understand cyber conditions, threats, and vulnerabilities, and clearly define how and where it can contribute to national cyberspace strategy. Furthermore, the Air Force must work toward consensus within the defense community on standardizing cyberspace definitions, doctrine, and operating concepts. Until these issues are fully addressed, the authors contend that the ability of the Air Force to develop, deliver, and employ sovereign and advantageous cyber operations will remain encumbered.

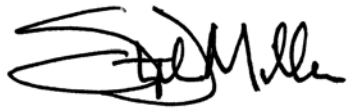
In support of Eighth Air Force requirements and the new Cyber Command, the study concludes with critical recom-

mendations to enable the Air Force to effectively "fly and fight" in cyberspace:

1. The Air Force needs a clearly articulated cyberspace operating concept, hardware and software tools, and a dedicated, trained Cyber Warfare Corps.
2. The Air Force should clearly define and distinguish the military operations and effects it expects to achieve with the signals, data, information, knowledge, and intelligence flowing through and resident in cyberspace.
3. The Air Force should understand the current US cyber situation, including cyber conditions, threats, and vulnerabilities.
4. The Air Force should select and systematically apply a methodology sensitive to the technology and transformation forces flowing from the information revolution in order to successfully plan strategy, build and organize forces, and resource its actions in cyberspace.
5. The Air Force should institutionalize "cyber-mindedness" and organize innovatively to successfully build capability and capacity for operating in cyberspace.

This study argues that these actions, taken together, will go a long way toward enabling war fighters to plan and execute cyber tasks, apply cyber capabilities, and integrate operations in cyberspace with military capabilities executed in the traditional war-fighting domains.

As with all other Maxwell Papers, this study is provided in the spirit of academic freedom and is open to debate and serious discussion of issues. We encourage your response.



STEPHEN J. MILLER
Major General, USAF
Commandant, Air War College

About the Authors

Lt Col Sebastian M. Convertino II is currently a senior planner for Air Force Cyber Command, Barksdale AFB, Louisiana. Prior to his current assignment, he was a student at Air War College, Maxwell AFB, Alabama. He has served as commander, 3rd Communications Squadron, Elmendorf AFB, Alaska, where he led Airmen and had responsibility for over $300 million in mission-critical communications assets. As an action officer assigned to the Joint Staff J-6, he served as principal author responsible for overhauling the joint requirements and interoperability systems. Additionally, he was aide-de-camp to the commander, Pacific Air Forces, Hickam AFB, Hawaii, and commanded the 406th Expeditionary Support Squadron, Taszar Air Base, Hungary, responsible for 175 Airmen who performed all mission-support functions. Colonel Convertino also served as both information and mission-systems flight commander at Royal Air Force Lakenheath, England, as well as chief, Red Switch Engineering, and executive officer to the director of technology and interoperability, Headquarters Air Force Communication Agency.

Lou Anne DeMattei is a senior intelligence officer with the Defense Intelligence Agency. She served on active duty for 10 years as a Navy cryptologic officer and continues her military affiliation as an officer in the Naval Reserve. She earned a bachelor of science degree in mathematics from the United States Naval Academy, a master of science in management from Troy State University, a master of science in strategic intelligence from the Joint Military Intelligence College, and a master of strategic studies from the Air War College.

Lt Col Tammy M. Knierim is the chief of Air Force Forces A65 Communications Plans Division at the combined air operations center at Al Udeid Air Base, Qatar. Her most recent assignments include deputy commander, 355th Mission Support Group, and commander, 355th Communications Squadron at Davis-Monthan AFB, Tucson, Arizona. She has served in positions at the base, group, wing, major command, and Air Staff levels. She earned a bachelor of arts degree at John Carroll University and received her commission through Officer Training School. She holds master's degrees in computer resources management, military operational

art and science, and strategic studies. Colonel Knierim is a graduate of Squadron Officer School, Air Command and Staff College, and Air War College.

Abstract

This research paper develops the foundation for a new military operating concept for "fighting the net" in support of Eighth Air Force's requirements and its stand-up as the new Cyber Command. It applies the Air Force Concept Development framework to examine cyberspace as a newly designated warfare domain and proposes cyber capabilities as well as effects that the Air Force should develop and apply as it seeks to execute its mission in cyberspace. Before the Air Force can effectively lead in the cyber domain, it must first not only fully characterize cyber conditions, threats, and vulnerabilities, but also clearly define how and where it can contribute to the national cyberspace strategy. Once the service completes these tasks, it can then focus on the nature of war in the cyber domain and consider the implications for military doctrine and operations. In order to successfully build capability and capacity for operating in cyberspace, the Air Force needs to institutionalize "cyber-mindedness" to underpin investments in organization, research and development, and human capital that it needs to "fly and fight" effectively in cyberspace.

Introduction

> *The use, reliance, and subsequent dependence on information and information systems in modern military conflict has created a new environment for competition . . . in a new medium with revolutionary implications. . . . Combat will take place in the physical space, in the cyberspace and in the perceptual space.*
>
> —Michael L. Brown, 1996

On 5 December 2005, the Air Force expanded its mission to include a new domain of war fighting: "to fly and fight in Air, Space, and *Cyberspace*."[1] This announcement recognized cyberspace operations as a vital national interest, essential to the conduct of joint military operations through the entire range of conflict. Having embraced cyberspace as a fundamentally distinct and physically unique operating domain, the Air Force has started to organize itself to conduct cyberspace operations. For its part, the Joint Chiefs of Staff, having formally established warfare requirements for the cyber domain more than a decade ago, published a standard definition for cyberspace in 2006.[2]

The measured evolution of cyberspace definitions, doctrine, organizations, and operating concepts is a testament to the complexity and uniqueness of this new military operational domain. It also recognizes the fundamental role that the information-technology revolution plays in driving the dynamics of this domain.[3] At the same time, the long lead time to formalize and standardize cyberspace operating concepts and definitions has given rise to a lack of conceptual as well as doctrinal clarity and consensus on the ends, ways, and means of operating in cyberspace; furthermore, it has resulted in an unfocused foundation on which to plan strategy, build and organize forces, and find resources for endeavors. Consequently, the ability to develop, deliver, and employ sovereign cyber options that achieve and maintain an advantage in the cyber domain—thus assuring information superiority—is encumbered. As a means to further evolve a conceptual foundation for "fighting the net," this research paper applies the Air Force Concept

Development framework to examine the unique attributes of cyberspace operations and propose a more focused definition of cyberspace.[4] In that context, it describes cyber capabilities and effects that the Air Force should develop and apply as it fully integrates existing and emerging technologies to ensure "freedom of cyberspace."[5] Finally, it assesses the conduct and character of war in cyberspace, offering recommendations for future cyberspace capabilities, policies, and military operating concepts based on that analysis.

The Cyber Dilemma

> *Mankind has always been aware of the existence and value of information. It took the invention of heavier-than-air machines to lead to a far greater exploitation of [air as a] dimension of strategy. Similarly, it may have taken the broader exploitation of the electromagnetic spectrum, and in particular the emergence of cyberspace, to realise fully the potential of information power.*
>
> —David J. Lonsdale
> *The Nature of War in the Information Age*

The Air Force recognized cyberspace as a fundamental war-fighting domain that hosts the bits and streams of data comprising basic building blocks of information, knowledge, and intelligence.[6] The Joint Staff's Joint Net-Centric Campaign Plan of October 2006 formally defined cyberspace as "a domain characterized by the use of electronics and the electromagnetic (EM) spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[7] This definition implied that cyberspace is broader than the EM spectrum alone and involves the use of data and hardware that channel EM energy to create an information environment. This definition implicitly bounds the problem set of cyberspace as informational and should lead the community to distinguish between information-based operations and energy- or signature-based operations (e.g., those employing directed energy, antiradiation, stealth, and cloaking technologies) and the synthesis of these in doctrine and operating concepts.

The defense community, however, holds a widely diverse range of views in defining military operations and effects involving the signals, data, information, knowledge, and intelligence flowing through and resident in cyberspace.[8] That diversity is reflected in differences in joint and service doctrine as well as in Department of Defense Directive (DODD) 3600.01, *Information Operations*, 14 August 2006.[9] Further, the set of activities currently identified as cyberspace operations by the defense community is considerably broader than those identified by other government agencies, the private sector, and the general population: outside the Department of Defense (DOD), cyberspace is understood to be the information environment enabled by the EM spectrum, rather than the energy environment created by the physical phenomenon of electromagnetism.

Additionally, fundamental inconsistencies exist among cyber objectives that describe effects the Air Force seeks to achieve through cyberspace operations: full-spectrum dominance, control of the information environment, or the "ability to secure the benefits of cyberspace" in order to deliver sovereign options—that is, assure "operational choices unlimited by distance and time" by means of shaping through strike and stabilization.[10] These inconsistencies have resulted in multiple organizational realignments, unfocused application of diverse and highly technical cyber skill sets, and lack of a clearly delineated career field for cyberspace operations in both the Air Force and its sister services. Further, these inconsistencies stymie cyberspace capabilities-based planning and complicate the development of synchronized operating concepts for the Air Force as it endeavors to man, train, equip, and apply a cyberspace force.

The Air Force has concluded that the cyberspace domain underpins every aspect of war fighting simultaneously at all levels of operations and that cyber capabilities are being rapidly developed as well as globally dispersed. However, its task of clearly and simply articulating what Airmen do in cyberspace and how they do it as war fighters remains. To clarify the task in terms of the newest joint parlance, the Air Force needs to determine how it will develop and apply cyber capabilities and conduct cyber operations that shape the environment, protect US interests, prevent surprise, and prevail against the enemy.[11] To better organize for this

task, the secretary and chief of staff of the Air Force established an operational command for cyberspace on 6 September 2006, announcing Eighth Air Force as the new Cyber Command.[12]

Bounding the Cyberspace Domain

A common understanding of the physical attributes of cyberspace and a clear delineation of the specific elements of military information operations (IO) that occur in cyberspace are necessary to enable a coherent description of missions and effects in the cyberspace domain. To provide a common foundation, we need to address several key questions:

1. What is the appropriate framework for understanding cyberspace as a war-fighting domain alongside traditional domains of war?
2. What are the physical attributes of cyberspace, and how are they similar to and distinct from traditional domains of warfare?
3. What specific elements of military IO occur in cyberspace?
4. What broad implications for joint military operating concepts result from the unique attributes of cyberspace?
5. What are the effects that one can and should consider in the cyberspace operational domain?

Requirement for a New Framework. Neither Air Force nor joint doctrine currently defines or distinguishes a cyberspace domain. The Air Force is fully ensconced in the challenge of pinning down standard, delimited, and consistent descriptions of cyberspace and cyberspace operating concepts. As a starting point, Air Force doctrine adopts a unique organizing construct for IO that includes the integrated employment of influence operations, electronic warfare (EW) operations, and network warfare operations—identified as "capabilities"—to be conducted in the cognitive, physical, and information domains of the "information environment."[13] In Air Force doctrine, cyberspace is generally understood as a host, in part, to

each of these IO domains. In joint doctrine, cyberspace is understood as a physical phenomenon distinct from the information environment, comprised of cognitive, physical, and information *dimensions*. Current IO doctrine and operating concepts blur the distinction between physical and nonphysical aspects of the "domain," fail to distinguish between "content" and "noncontent" actions on data and information, and combine what are essentially both methods and effects under the rubric of "capabilities." Consequently, current doctrine is limited in its ability to provide a clear and delimited organizing construct for development of synchronized application (ways) of cyber capabilities (means) to achieve desired effects in both cyberspace and other domains (ends). Nonaligned effects require functionally diverse capabilities. They complicate the development of cyber capabilities as well as cyber-related organizational management.

To illustrate, table 1 provides a mapping of IO effects (ends) currently identified in joint doctrine against representative ways and means of achieving those effects. The clustering of computer network operations (CNO), spectrum management, and signal processing "means" for noncontent signal and data effects is largely distinguishable from means for content data, information, knowledge, and intelligence effects (i.e., information management, perception management, and interdisciplinary information effects).

To better enable development and integrated application of cyber capabilities (means), we need to describe cyber effects in a more streamlined fashion for both offensive and defensive applications. For example, the elements of information assurance (IA), used in combination with a distinct set of information and perception-management effects, could provide a more usable model for applying integrated means that achieve IO ends (table 2). Similar to the IA construct, the Air Force Research Laboratory uses the seven-layer Open System Interconnect model and transmission control protocol / Internet protocol (TCP/IP) as an architecture to guide its research and development of cyber capabilities.[14] Taken together, these illustrations show that one can describe a more homogeneous set of cyber means to achieve effects (ends) that are functionally aligned.

Table 1. Mapping of ways and means to IO ends

Ends	*Ways*	*Means (Noncontent)*	*Means (Content)*
Effects to be achieved in any war-fighting domain	*Synchronized application of capabilities*	*Capabilities to affect signals and noncontent data actions*	*Capabilities to affect content data, information, knowledge, intelligence/insight actions*
Destroy system		Physical destruction of system or data (e.g., format hard drive)	Not directly applicable as a first-order activity
Disrupt information		CNOs, signal processing, and EM spectrum management	Not directly applicable as a first-order activity
Degrade command and control (C2) / C2 systems and information-collection means		CNOs, signal processing, and EM spectrum management	Not directly applicable as a first-order activity
Deny access to critical information, systems, and services		CNOs, signal processing, and EM spectrum management	Not directly applicable as a first-order effect
Deceive (military deception [MILDEC])	Apply non-kinetic (cyber) capabilities as a principal method of offensive or defensive operations	Not directly applicable as a first-order activity	Perception management achieved through data and information manipulation
Exploit C2 by gaining access to systems		CNOs	Information management
Influence adversary behavior		Not directly applicable as a first-order activity	Interdisciplinary
Protect against espionage or capture		Information management (communications security)	Interdisciplinary (counterintelligence, information security, physical security)
Detect system intrusion		CNOs	Not directly applicable as a first-order activity
Restore information / information systems to original state		CNOs	Not directly applicable as a first-order activity
Respond to adversary attack or intrusion		CNOs	Not directly applicable as a first-order activity

Source: See Joint Publication 3-13, *Information Operations*, 13 February 2006.

Table 2. Mapping of ways and means to IO ends (IA elements)

Ends	*Ways*	*Means*	*Means*
Effects to be achieved in all war-fighting domains	*Synchronized application of capabilities*	*Capabilities to affect signals and noncontent data actions*	*Capabilities to affect content data, information knowledge, intelligence/ insight actions*
Authentication		Not applicable as a first-order activity	CNOs
Availability	Apply non-kinetic (cyber) capabilities as a principal method of offensive or defensive operations	CNOs, signal processing, and spectrum management	CNOs
Confidentiality		CNOs	CNOs
Integrity		CNOs	CNOs
Nonrepudiation		CNOs	CNOs

Physical Attributes. At a basic level, cyberspace shares some important characteristics with traditional domains of war. To cite a simple but illustrative analogy, cyberspace is a physical phenomenon (the EM spectrum and data activities) that serves as a host and medium for implements of war (digital representation of data, information, knowledge, and intelligence; electronic systems and networks; and cyber craft), much the same as the land hosts ground implements of war (soldiers, tanks, and guns), the sea hosts maritime implements of war (sailors, ships, and missiles), and the air and space host airborne weapons of war (airmen, fighters/ spacecraft, and missiles/lasers).

Like other domains, cyberspace is global. It hosts a full range of societal activities (one of which is war fighting), and it can serve as a medium through which both kinetic and nonkinetic effects are delivered, using both noncontent and content actions. In relationship to the other domains, cyberspace is unique in its physical characteristic as a medium through which operations across all war-fighting domains are coordinated, synchronized, and integrated—and its global reach is immediate. Unlike operating concepts for applying air, space, maritime, and land power, time and

distance constraints decrease exponentially in the physical application of cyber power.

One can create data, the basic resource of cyber power, at will; it is essentially unlimited and unconstrained as a "material" component of warfare. Data itself can have veracity; at the same time, it can be wholly or in part contrived in its representation of information, knowledge, and intelligence (and thus can be used to create a "fictive" universe)—a material component of the cognitive domain used to create influence effects.[15] Unlike most material components of other operational domains, some of the data and information relevant to war fighting that reside in cyberspace are much more difficult to distinguish from data and information used in other societal activities.

The central challenge of war fighting in cyberspace thus becomes the war fighter's ability to command, control, and manage a near-infinite, temporally rapid component (digital data) in establishing and applying force capabilities—reach, agility, presence, situational awareness, power projection, domain control, and decisive force—to achieve desired effects across the spectrum of war. This C2 task must increasingly occur in real time, not only at the signal and data levels but also at the information, knowledge, and intelligence levels. Because of the central role of the network in modern warfare and these unique physical attributes, both the content and the flow of data need to be characterized as distinct operational functions in organizational frameworks that support development of new cyberspace operating concepts.

Domain Differentiation: Cyber versus Information Operations in Cyberspace. Based on this characterization, we can now articulate a more succinct distinction between military IO activities that occur in the cyberspace domain and the EM spectrum. The association of "military activities" within a specific war-fighting domain is a generalization that helps to conceptualize and plan; it is not intended to be exclusive. For example, although the bulk of maritime operations takes place in the physical environment of water, obviously not all water-based maritime activities are naval-warfare operations—for example, port operations and law-enforcement activities. Similarly, although the bulk of cyber operations takes place in the physical environment of the EM spectrum, we should not char-

acterize all EM-based military activities as cyberspace operations. Nor should we characterize all military activities that take place in what we currently refer to as the information environment—conceptualized as a compilation of the physical, cognitive, and informational domains—as IO unless they directly involve the cognitive, content aspect of data and information.[16]

Air Force IO doctrine identifies three domains in which IO is conducted (physical, information, and cognitive) and three distinct types of IO (influence operations, network warfare, and EW). Doctrine suggests that influence operations primarily occur in the cognitive domain of cyberspace, network-warfare operations in the information domain, and EW (primarily) in the EM spectrum (which, by the current definition, is the cyberspace domain). As such, the physical domain of cyberspace is used to dictate the operational classification of activities occurring there as information activities even though they are technologically disparate, loosely related as functions, and—as in the case of EW—not all information-based. This paper takes the position that cyber operations be designated as a mission activity focused primarily on noncontent operations involving content-based digital data and data flow. This mission category would encompass most network-warfare operations and only a limited subset of information-based operations (occurring in the cognitive domain)—as well as a limited subset of EW operations (occurring in the EM spectrum). We should broadly redefine the term *influence* as an effect achieved through the application of all types of military activity since almost all military operations have a role in influencing adversary/target-audience decision making as a first- or second-order effect. Likewise, we should address EW separately as a noncontent, energy-based activity rather than as an IO activity—as is currently the case.[17]

To address the definitional, consistency, and complexity dilemma, one may propose a new conceptual framework for cyber operations within seven operational domains of war, one of which is cyberspace (table 3). This construct adopts a narrow definition of cyberspace operations focused on CNO actions on content data, as distinguished from operations involving derivative informational resources that reside, in part, in cyberspace (information, knowledge, and intelligence), as well as signature-based and energy-based activities that also occur in the EM spectrum. An operational example of this

type of organizing construct is used at the National Security Agency (NSA), which categorizes its signals-intelligence operations as communications intelligence (communications signals), electronic intelligence (electronic/noncommunications signals), foreign instrumentation signals intelligence (telemetry), and a small number of hybrids; further, for a range of functional and programmatic reasons, it maintains a separate IA directorate for CNO defense and related activities. The taxonomy has proven highly useful for manning, training, organizing, and equipping the NSA's signals-intelligence and IA forces. Like the NSA model, table 3 distinguishes between informational- and energy-based activities occurring in the EM spectrum, associates the cyberspace domain with noncontent data and information actions in the information environment, and distinguishes a cognitive domain for information and perception-management activities (that are enabled in part, as are all other non-EM domain activities, by the EM spectrum).

Table 3. Cyberspace in a conceptual framework for war-fighting domains

Physical Environment	Vacuum	Gas	Solid	Liquid	Multimode	Multimode	Decision/ decision-support hosts
Operational Domain	Space	Air	Ground	Maritime	Cyberspace	EM spectrum	Cognitive
Missions/ Activities	Space operations	Air warfare	Land warfare	Naval warfare	Cyber (digital data) operations (CNOs)	EW (signal processing, EM spectrum management, directed-energy operations)	Information and perception-management operations
Effects	Kinetic and nonkinetic capabilities applied to achieve dominance, control, superiority, freedom of operation/access, and influence (adversary decision making) through offensive and defensive operations						
Sample Material Components	Satellites	Fighters	Tanks	Ships	Digitized data, networks, and networked systems	Digital and analog energy streams and systems	Digital, analog, printed/ recorded/ retrievable information
Sample Organizational Elements	Space Command	Air operations center	Third Infantry Division	Sixth Fleet	Cyberspace Command	Army Electronic Warfare Division	Fourth Psychological Operations Group

As a concluding caveat on framework, it is important to consider the role and state of technology in the proposed construct. Table 3 emphasizes a TCP/IP-centric differentia-

tion for cyberspace because it is most consistent with state-of-the-art and state-of-practice applications. Energy-based EW is not currently TCP/IP-based but might become so in the future. Likewise, when technology creates a truly "non-biological-human decision-making" hybrid, as envisioned by renowned scientist and futurist Ray Kurzweil, one may very well better conceive the cognitive domain as a subset of cyberspace or the EM spectrum domains.[18] However, until such syntheses render differentiation irrelevant, explicit domain distinctions of cyberspace and the EM spectrum, as well as the primary military operations that occur in these domains, will better support and facilitate development, organization, resourcing, and staffing of cyber capabilities.

Broad Implications for Joint Military Operating Concepts. The characteristics of cyberspace as a host for integrated, networked data and information relatively unbounded in time, distance, and volume have specific doctrinal and operational implications. At the macrolevel, cyberspace, its resources, and the activities occurring in and enabled by cyberspace that bear on national security are not predominantly military. Cyber warriors will be increasingly challenged to distinguish what they should and should not conduct as military activities in cyberspace, and cyber operating concepts will increasingly need to be integrated and synchronized with the activities of nonmilitary organizations that share cyberspace and support national security missions. Further, even in military operations, cyber operations are emphasized apart from EW as nonkinetic, noncombat "shaping" and "intelligence preparation of the operational environment" functions employed throughout all campaign phases.

The cognitive, physical, and information-domain bins currently used to describe an information environment in which influence, network warfare, and EW operations occur are limited as a construct in helping to conceptualize and plan what war fighters do in cyberspace. Because current doctrine groups these functions as IO, our ability to integrate and apply their distinct capabilities in a logical, sequential, and integrated manner is often underemphasized—sometimes ignored. For example, Gen Ronald Keys, chief of Air Combat Command, made the following observation regarding potential application

of F-22s as intelligence collectors supporting counter-insurgency operations in Iraq:

> You've got to turn down the sensitivity. . . . I don't think it's a fatal flaw, but we now realize that in some situations we may not be able to see some of the [intelligence] we wanted to because we simply jam it off the air.
>
> We didn't anticipate there was going to be this level of jamming. Every patrol is out there with personal jammers. We've got lots of airplanes that are also jamming. At the same time, we've got people trying to listen [to insurgent conversations], a lot on the same or overlapping frequencies.[19]

Most experts find that the emergence of cyberspace, along with the information and networked environments that it enables, lays the groundwork for a revolution in military affairs (RMA). A smaller number of experts believe that cyberspace will eventually result in a fundamentally new approach to warfare. Jeffrey R. Cooper's levels of impact for information warfare (fig. 1) offer perhaps one of the best illustrations of this notion. The model examines logically grouped, information-based capabilities, methods, and effects to describe three levels of impact that the "information revolution" has had at the tactical, operational, and strategic levels of information war. This is a particularly useful construct because it distinguishes, correlates, and clarifies EM- and cognitive-based activities executed in the cyberspace domain. Cyberspace implications for the RMA are further detailed in the section "Recommendations on the Way Ahead."

Effects in Cyberspace. The proposed conceptual framework identifies cyber operations as a CNO mission-level activity. As such, basic cyber capabilities should include cyber intelligence, surveillance, and reconnaissance (ISR), cyber defense, and cyber attack, using tools and approaches such as cyber craft and defense in depth. Corresponding cyberspace operations include network modeling and indications and warning; attack protection, detection, attribution, and reconstitution; and access denial, system degradation, and data destruction. The effects that cyber operations should have in achieving strategic and operational objectives as well as protecting US interests should then include

1. knowledge of adversary networks and nodes to prevent surprise in cyberspace;

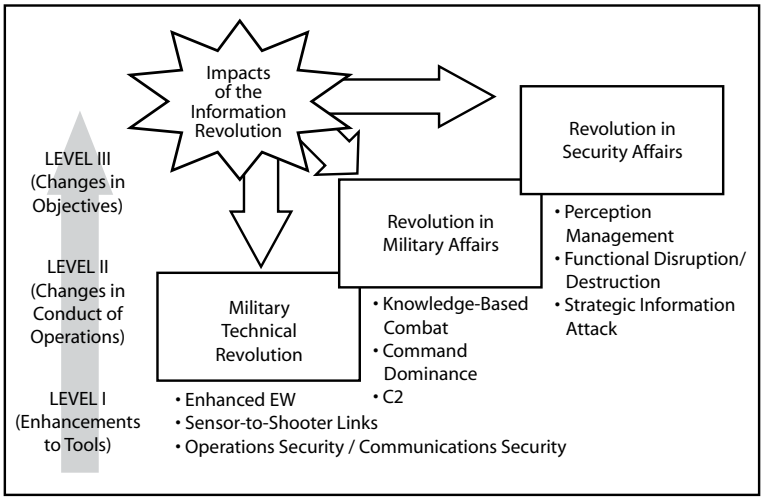


Figure 1. Levels of impact for information warfare. (Reprinted from Jeffrey R. Cooper, "Another View of Information Warfare," in *The Information Revolution and National Security: Dimensions and Directions*, ed. Stuart J. D. Schwartzstein [Washington, DC: Center for Strategic and International Studies, 1996], 125.)

2. assurance of systems and ability to operate in and shape the cyberspace environment; and
3. military operational advantage in cyberspace to influence, engage, and prevail against the enemy in the cyberspace domain.

One can achieve strategic and operational objectives to assure information power in cyberspace, as well as enable the exercise of military power and superiority in other domains, through streamlined application of cyber capabilities fully integrated, with other types of military operations.

Implications for Command and Control, Network Operations, and Intelligence, Surveillance, and Reconnaissance

C2 and network operations are both largely conducted in and dependent on cyberspace. A decision-making activity rather than a data activity, C2 should be considered a cognitive function—not a cyber capability. Network operations—

essentially an IA activity provided through network defense—are a basic task enabled through cyber-defense capabilities. C2, network operations, and ISR are presently characterized as "integrated control enablers" of IO.[20] Current organizational constructs, as well as service, budgetary, and regulatory authorities, drive this characterization rather than apply classification based on their functionality and capabilities as military activities. In January 2007, the Air Force chief of staff announced plans to consolidate all ISR programs under a new Air Force ISR command for the purpose of addressing alignment of integrated, control-enabling resources and capabilities.[21] Both the Army and Navy are also involved in operational-alignment activities involving cyber, communications, and intelligence capabilities and organizations.

A New Military Problem and New Solutions

The ability to fly and fight effectively in cyberspace now and in the future hinges directly on the proper definition, scope, conceptualization, and integration of tasks, effects, conditions, and objectives of operating in cyberspace.[22] The military problem of fighting in that realm is new in that it fundamentally involves a nonkinetic, nonviolent approach to war. The basically new—or at least underdeveloped—military problem in the cyber domain entails scoping military application of cyber operations—and doing so primarily as a nonviolent force application of cyber tools in the weapons arsenal. Cyber capabilities can assuredly support application of other force capabilities, but, fundamentally, they are not the destructive, kinetic purveyors of violence that war fighters traditionally envision in planning military strategy, engagements, and war. If we apply them as primary weapons of war, then basic concepts regarding the use of force or threat of force to compel the enemy must change. On the surface this approach appears straightforward, but it should prompt careful consideration of how the character and conduct of war differ in cyberspace.

Cyber capabilities developed as weapons for fighting the net exist in a parallel, mostly integrated, and nonmilitary part of cyberspace; they represent a second key consideration. This cyberspace slice is not necessarily distinguishable from a joint cyber-operations area of war; furthermore,

many cyber weapons remain indistinguishable from those capabilities applied as tools of nonmilitary network management, societal informational activities (e.g., governmental, economic, political/ideological, and religious), technology sharing, criminal activities, or even vigilante activities and thrill seeking on the net. For example, one has difficulty envisioning a routine civil application of a missile, but it is entirely conceivable that commercial entities deploy cyber craft that collect against and target audiences to influence their behavior—the same cyber craft that would be applied in similar manner (potentially against the same targets) by the military as weapons. Essentially, cyberspace is a shared domain; cyber capabilities are inherently nonviolent weapons coexisting as tools in much of human activity.

Missions That Assure Operations in Cyberspace. In view of the unique attributes of cyberspace and the nature of cyber weapons, it is appropriate to identify cyber missions that provide dominance, superiority, decisive control, and sovereign options in cyberspace.[23] Such understanding and characterization will drive organizational constructs, resources, and processes that develop and deliver cyber capabilities.

The 2005 *National Defense Strategy of the United States of America* established a requirement for capabilities that enable operational freedom of action in cyberspace as a part of the "global commons," linking the success of military operations with the ability to protect information infrastructure and data and to counter an adversary's exploitation of network vulnerabilities—in essence, to "assure" the ability to operate in cyberspace.[24] Secretary of the Air Force Michael Wynne further addressed this issue directly in remarks during a conference in November 2006 by offering a powerful analogy between freedom of the seas and freedom of cyberspace. His message identified the overarching missions to be conducted in cyberspace:

1. Sustain military action to ensure freedom of access and usage of cyberspace.
2. Prevent illicit use of cyberspace.
3. Maximize access to and ensure veracity of data residing in cyberspace in order to secure the benefits of

this domain for the military, as well as other national interests.[25]

Taken together, these missions emphasize an overarching strategic approach that can be characterized as a military requirement to maintain a steady-state of "global assured operations," with the more traditional force-application concepts of dominance, superiority, and decisive control reserved for the tactical and operational cyberspace activities associated with specific military campaigns and operations.

Time Horizon, Assumptions, and Risks. The target time frame for operating concepts suggested by this study is 2009–14, in order to enable programmatic planning that applies period-relevant assumptions and risks based on state-of-the-art and present-state technology considerations. Common assumptions about the nature of cyberspace introduce risk to implementation feasibility. These assumptions include the concept of boundaries, control, and defense of cyberspace; characterization of cyberspace and information as a US center of gravity; and technology development and research resourcing.

Although establishing boundaries in cyberspace as a global domain may or may not prove feasible, doing so may be an essential task required to effectively perform the military functions of control and defense of cyberspace. Disparate expert opinions exist on the concept of boundaries in cyberspace. Citing the *National Military Strategy for Cyberspace Operations* of 2006, Dr. Lani Kass, director of the Air Force Cyber Task Force, found that boundaries do not apply in cyberspace and that control of cyberspace is an essential task of the Air Force cyber mission.[26] Dr. Martin Libicki, renowned policy expert on the RMA and information warfare, asserted that cyberspace is ubiquitous, neither owned nor defendable by the DOD acting alone. As a result, he finds that the concept of forcible entry does not exist in cyberspace in the same way it does in other warfighting domains.[27] Dr. David Lonsdale, expert in international relations and information warfare, found that cyberspace and the information resident in it are increasingly becoming "territorialized" and therefore will eventually be controlled and defended.[28] In contrast, consider the very viable endeavors of *Wikipedia*, the Open Software Initiative,

and Dr. Robert David Steele's concept of open-source intelligence, which together demonstrate an open architecture for data, information, knowledge, and intelligence.[29] Given the range of expert opinions, one can only conclude that the jury is still out on the concepts of boundaries, control, and defense in cyberspace. Therefore, developing, resourcing, and applying military cyber capabilities that either assume boundaries or unrealistically assume the possibility of global control are at risk. This risk is further amplified by the dynamic nature of cyberspace as well as the virtually unlimited capability to create new data and resources targeted by cyber military operations.

Conventional wisdom holds that cyberspace and the information residing in it constitute a US center of gravity. Dr. Joe Strange, strategy and campaign-planning expert, postulated that centers of gravity must have the ability to "strike heavy or effective blows, and must offer resistance."[30] A metaphor for cyberspace and information as a center of gravity that meets these criteria is difficult to conceive, but it is relatively easy to describe belief systems and their decision makers as such. Given this more nuanced understanding of the characteristics of a center of gravity, we may need to reconsider conventional wisdom regarding cyberspace and information as a center of gravity.

Technology assumptions also pose a significant risk. Breakthrough developments and new applications in cyberspace are both possible and difficult to predict. Given the pace and volume of technology development, profound changes in cyber capabilities could emerge rapidly. For example, breakthroughs in areas such as quantum cryptography and nanotechnology could render current notions of secure electronic transactions obsolete. Resourcing and focus of research—closely related to technology assumptions—should drive risk considerations.

Relevance

Clarity of words, definitions, and concepts is important and relevant. Simply put, war fighters must fully embrace cyberspace as a war-fighting domain. They must have confidence in planning and executing cyber tasks, applying cyber capabilities, and integrating operations in cyberspace

with other domains in order to achieve intended effects. Until we can clearly conceptualize and describe this domain and operations in it, we cannot offer a viable, effective road map for the development and application of cyber capabilities. War fighters will neither embrace nor realize the full benefit of cyber power, and, worse, we will risk missing or losing completely the opportunity to seize and maintain the advantage of the cyber operating environment.

Proteus, a project sponsored by the National Reconnaissance Office, examined the "problem space" of the future to inform the intelligence community of its projected national security roles in the 2020 environment. It describes "planes of influence"—terrestrial, space, spectral, virtual, and psychological—to replace traditional war-fighting domains. Proteus postulates that the Internet has enabled a fundamentally new kind of "mutable knowledge" that renders the concept of a network inadequate for defining and understanding IO. It proposes conceiving of the Internet as a parallel universe rather than simply a global network. To paraphrase *Proteus: Insights from 2020*, for untold millennia, epistemology has held that knowledge arises from three sources: authority, empiricism, and revelation. For the first time in human experience, a fourth kind of knowledge may be arising. Complex, interconnected global networks can lead to the spontaneous creation of knowledge. The speed with which the new knowledge is created and disseminated is nothing short of remarkable. The new knowledge remains silent regarding intrinsic truth or falsehood. In the progression from data through knowledge to insight, understanding what is knowable may prove more important than differentiating between truth and falsehood.[31]

The cyberspace universe of 2020 is rapidly approaching. In the meantime, it is imperative to start small and at the beginning. We must clearly understand the digital-data environment; data constructs, tools, applications, and transport; and ways of knowing and using data in the context of offensive and defensive military operations. Only then will an adequate conceptual foundation become available to properly evolve future operating concepts for flying and fighting in cyberspace.

The US Cyber Situation: The Perfect Storm?

A strong disturbance associated with a cold front moved along the U.S.-Canadian border on October 27, 1991 and passed through New England pretty much without incident. At the same time, a large high-pressure system was forecast to build over southeast Canada. When a low pressure system along the front moved into the Maritimes southeast of Nova Scotia, it began to intensify due to the cold dry air introduced from the north. These circumstances alone could have created a strong storm, but then, like throwing gasoline on a fire, a dying Hurricane Grace delivered immeasurable tropical energy to create the perfect storm.

—Robert Case
National Weather Service, Boston

The perfect storm described above is also known as the Halloween Nor'easter of 1991. This storm devastated the Atlantic seaboard for days, killed 12 people, and resulted in over $1 billion in damage. The storm was not a hurricane, so it did not elicit the normal hurricane warnings. Therefore, it caught many onshore citizens and deep-sea fishermen off guard. Had any of the events that contributed to this storm changed, the overall impact would not have been so devastating.

A perfect storm involves the convergence of independent events that form an environment never before experienced. The current US cyber situation involves diverse threat agents that, if conflated with system vulnerabilities, will create the cyber perfect storm. Unless we put into practice national strategies and policies to change one or more of these contributing factors, the US cyber perfect storm will have effects that go far beyond property damage and shoreline erosion.

When Air Force leadership revised the service's mission statement to say "fly and fight in air, space, and *cyberspace*," it signed up to tackle these existing threat agents and system vulnerabilities. However, before the Air Force

can effectively lead in the cyber domain, it must first fully understand the current US cyber situation that points to the perfect storm. The service must examine threat agents, dissect current vulnerabilities, prioritize credible threats, and clearly define how and where it can contribute to the national cyberspace strategy.

The following sections note current conditions in the cyber domain, highlighting key definitions and assumptions. The next part examines cyber threat agents as existing weather fronts and provides evidence identifying current US cyberspace vulnerabilities—the "strong tropical disturbance feeding energy to the fronts." After building the case for an impending perfect storm, the final portion explores the US strategic way ahead that is battling the "simultaneously challenging winds of change." Together these elements define the current US cyber situation and point toward a perfect storm.

Current Conditions in the Cyber Domain

> *The country's problem with cyber security is very serious, and it is going to get worse in the next five years before it gets any better. I would say the situation not only is alarming, but it is almost out of control.*
>
> —Clifford Lau
> Chair, Institute of Electrical and Electronics Engineers-USA's Research and Development Policy Committee

Weather forecasting concerns itself with analysis and interpretation of the evolution of atmospheric phenomena. As such, the science of weather forecasting relies on certain definitions and assumptions. Because accurate forecasting in the cyber domain resembles weather forecasting, it is useful to provide a brief synopsis of the current environment in the cyber domain. The US information infrastructure is defined as interconnected computing and storage systems, mobile devices, software, wired and wireless networks, and related technologies.[32] Before examining threats to this infrastructure, we outline certain assumptions about the cyber domain in table 4 to provide a common reference point for discussion.

Table 4. Key assumptions about the cyber domain: current conditions

☑	Information-technology infrastructure is indispensable to public- and private-sector activities across the globe.
☑	Interconnectivity exposes previously isolated critical infrastructures to the risk of cyber attacks mounted through the information-technology infrastructure by hostile adversaries.
☑	Exposure to attacks is expected to rise as convergence of network and device technologies accelerates and as systems increasingly connect to the Internet.
☑	Resources for potentially harmful attacks are readily available and relatively inexpensive.
☑	Adversaries are capable of launching harmful attacks on US systems, networks, and information assets.
☑	Individuals and organizations worldwide can access systems and networks connected to the Internet across geographic and national boundaries.
☑	Sensitive information tends to be isolated from the Internet, but the various gateways that exist to facilitate transfer of information from the outside into a closed network provide many openings for possible attack.
☑	Safeguarding the US information-technology infrastructure and critical infrastructure is a matter of national and homeland security.

Source: Data compiled from various reports of the National Science and Technology Council, Government Accountability Office, Center for Strategic and International Studies, and President's Information Technology Advisory Committee as well as the Department of Homeland Security's cybersecurity strategy and the *National Strategy to Secure Cyberspace*.

Undoubtedly, increasing computer interconnectivity has revolutionized the way that much of the world communicates and conducts business. Although benefits from this globalization are extensive, this interconnectivity brings with it risks to everyone, from the home user to large corporations and the federal government. The increased availability of tools for those who would choose to do harm, high-speed rate of technological advances, and increased global dependence on this interconnectivity escalate the risk.

It is important at this point to distinguish between the definition of the US information infrastructure and the US critical infrastructure. The USA Patriot Act, section 1016, defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security,

national public health or safety, or any combination of those matters."[33] Table 5 provides a list of the 14 US critical-infrastructure sectors with their designated lead agency.

Table 5. US critical-infrastructure sectors with lead agency

Critical Infrastructure Sector	*Lead Agency*
Agriculture	Department of Agriculture
Food	Meat and poultry: Department of Agriculture All other food products: Department of Health and Human Services
Water	Environmental Protection Agency
Public health	Department of Health and Human Services
Emergency services	Department of Homeland Security (DHS)
Government	Continuity of government: Department of Homeland Security Continuity of operations: all departments and agencies
Defense industrial base	DOD
Information and telecommunications	DHS
Energy	Department of Energy
Transportation	DHS
Banking and finance	Department of the Treasury
Chemical industry	Environmental Protection Agency
Postal and shipping	DHS
National monuments and icons	Department of the Interior

Source: Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Government Printing Office, July 2002), 32, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

Table 5 shows that the US critical-infrastructure sectors are substantial, composed of both private and public entities. The *National Strategy to Secure Cyberspace* states that the common thread linking these diverse sectors is the domain of cyberspace—the "nervous" system that "controls the country."[34] It is this nervous system that requires national vigilance and safeguarding. These definitions and assumptions offer a starting point to begin forecasting incoming fronts by identifying and analyzing threat agents.

Existing "Weather Fronts": Cyber Threat Agents

Fronts are boundaries between air masses of different temperatures that extend horizontally and vertically. In or-

der to create a strong storm, another force must strengthen these fronts. Similar to a typical weather front, current cyber threat agents manifest themselves from every direction, anxious to receive energy in order to intensify and build into a much stronger storm. Much like successfully forecasting an incoming weather front, if the Air Force wishes to become effective in flying and fighting in cyberspace, it must anticipate, assess, and prioritize cyber threat agents.

Threat and Threat Agent Defined. According to the Interagency Working Group on Cyber Security and Information Assurance, a cyber threat is "any circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a system resulting in a loss of confidentiality, integrity, or availability."[35] As defined here, cyber threats not only involve an action but also require actors (threat agents) to execute that action in order to exploit cyber weaknesses.

Profiles of Threat Agents. Threat agents, those people or organizations who intend to exploit vulnerabilities, represent a huge growth industry. The frequency of cyber attack incidents has become so commonplace that the US federal government's center of Internet-security expertise, the Computer Emergency Readiness Team, ceased reporting the number of incidents in 2004 because the overwhelming numbers provided little information to help assess the scope and impact of attacks.[36] From 1988 through 2003, over 319,000 incidents were reported. More alarming is that these incidents may have involved one site or hundreds or even thousands of sites. Figure 2 depicts the dramatic rise in *reported* incidents.

The data in the figure clearly indicates that both the frequency and effectiveness of malicious cyber attacks are escalating. One can place the threat agents executing these attacks (who are evolving as they multiply) into four general profiles: hackers, organized crime, terrorists, and nation-states. Table 6 provides a brief synopsis of threat agents together with their methodologies and intent.

The most widely discussed category of threat agents—hackers—possesses a collection of skills that allows them to break into systems for the simple challenge of the act or for more malicious intent. They may use either their own code or easily accessible scripts to launch attacks or

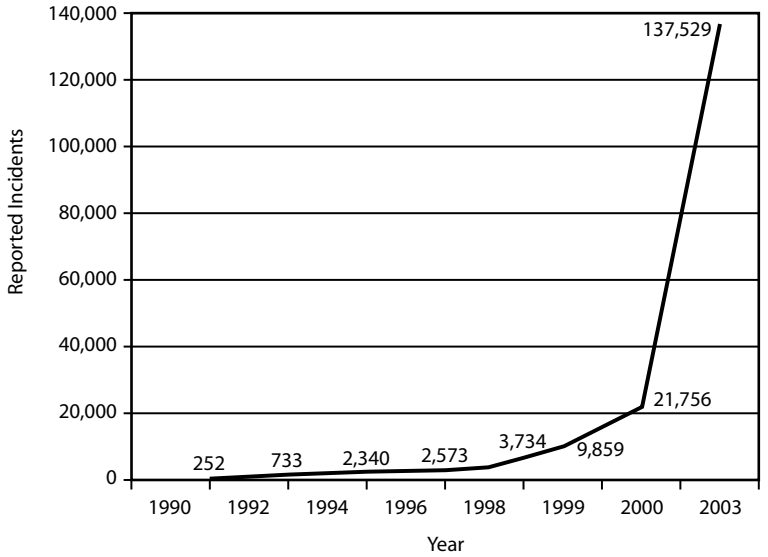


Figure 2. Reported security incidents, 1990–2003. (Data compiled from the US Computer Emergency Readiness Team, http://www.cert.org.)

Table 6. Synopsis of threat agents, methodologies, and intent

Threat Agent	*Methodology*	*Intent*
Hackers	☒ Develop/use damaging code to break into private networks	☒ Malicious or criminal intent Theft, fraud, denial of service, and extortion
Organized crime	☒ Exploits online activity, hires hackers, bribes insiders Uses more structure/resources than hackers	☒ Monetary gain
Terrorists	☒ Hacking Exploitation of Internet	☒ Acquire information for planning physical or cyber attacks C2
Nation-states	☒ Offensive cyber capabilities Technical and operational capabilities for widespread impact limited to only a few	☒ Espionage Cyber warfare

Source: Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Government Printing Office, July 2002), passim, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

probes. Types of hackers include botnet operators, phishers, and spammers, to name a few. Botnet operators take over several systems to allow coordinated attacks at a time of their choosing or at a time of their client's choosing. Phishers execute scams aimed at stealing identities or information for monetary gain. Spammers may include individuals or groups that distribute unwanted e-mail with hidden information to sell products, conduct phishing scams, or implant spyware.

Recognizing that hackers have the potential to perform tasks leading to monetary gain, organized crime is increasingly recruiting hacking services. The FBI's Internet Crimes Complaint Center reported in 2005 that it processed over 228,000 cyber-crime complaints, referred nearly 100,000 cases for criminal investigation, and estimated the total loss from fraud at $183 million.[37] These types of events involve tools ranging from spyware/malware, hacking, and phishing to spam. Although much of the reported malicious cyber-crime activity is not aimed at agencies or departments of the federal government, the significance of these cyber trends is their frequency and increasingly sophisticated tools and methods. These "commodity" hacker tools and methods are also readily available to terrorist groups and/or nation-states—the types of adversaries the Air Force will most likely face in the cyber domain.

Terrorist groups such as al-Qaeda are increasingly looking toward the cyber domain as an avenue to achieve their goals. Osama bin Laden was quoted as saying that "it is very important to concentrate on hitting the U.S. economy through all possible means."[38] Evidence of terrorist organizations' awareness and use of information technology and the cyber domain has grown since 2000. As physical and border security increases, terrorists may turn to cyber warriors or hacker services to engage in cyberterrorism against the United States.[39]

The FBI defines cyberterrorism as "a criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or

population to conform to a particular political, social or ideological agenda."[40] Although some debate exists about whether true cyberterrorism is a near-term or long-term possibility, increasing technical competency in terrorist and other groups is resulting in an emerging capability for network-based attacks.

Terrorist groups currently lack the required resources, skill, and coordination to conduct large-scale cyberterrorism; nevertheless, traditional nation-states are actively building both offensive and defensive capacity to execute cyber warfare. According to a Congressional Research Service report, one can use the term *cyberwarfare* to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same.[41]

We previously discussed the concept of cyberspace and the information residing in it as possibly constituting a center of gravity. Although this argument will be debated for some time, current evidence indicates that the cyber domain is quickly becoming a focus for nation-states in posturing themselves for future warfare. John A. Serabian Jr., IO issue manager for the Central Intelligence Agency, testified before Congress that

> we are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. We have identified several, based on all-source intelligence information, that are pursuing government-sponsored offensive cyber programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks.[42]

Clearly, foreign governments are postured to conduct structured attacks because of their access to technology, intelligence, funding, organized doctrine, and willingness to subscribe to longer-term goals and objectives.[43]

In 2004 the DHS provided a grant to the Institute for Security Technology Studies to assess potential foreign computer threats to information-technology networks in the United States. The study focused on overseas cyberthreat capabilities in order to dispel myths about the nature and degree of such a threat. Countries scrutinized include China, India, Iran, North Korea, Pakistan, and Russia (table 7).

Table 7. Summary of cyber capabilities of certain nation-states

	China	*India*	*Iran*	*North Korea*	*Pakistan*	*Russia*
Official cyber-warfare doctrine	X	X			Probable	X
Cyber-warfare training	X	X	X		X	
Cyber-warfare exercises/ simulations	X	X				
Collaborating with information-technology industry and/or technical universities	X	X	X		X	X
Information-technology road map	Likely	X				
Information-warfare units	X	X		X		
Record of hacking other nations						X

Source: Charles Billo and Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (Hanover, NH: Institute for Security Technology Studies, Dartmouth College, December 2004), passim, http://www.ists.dartmouth.edu/projects/archives/cyberwarfare.pdf.

The preceding discussion has illustrated the fact that cyber threat agents exist, take many forms, and are becoming stronger every day. Without a doubt, malicious cyber activity has increased dramatically and continues to proliferate. Having defined and assessed cyber threat agents as "incoming weather fronts," we should now examine vulnerabilities that feed these threats.

Strong Tropical Disturbance Feeding Energy to the Weather Fronts (Also Known as Cyber Vulnerabilities)

In addition to tracking the moving weather fronts, a vigilant forecaster must watch for potential weather patterns that have the potential to merge with and strengthen the storm. A strong tropical disturbance is a discrete system of organized showers and thunderstorms with tremendous energy. Combining this energy with existing weather fronts in the right conditions can create remarkable storms. Forecasters must not only monitor the weather fronts but also watch these other weather patterns that could collide with and intensify the front.

Current US cyberspace vulnerabilities provide possible sources of additional energy to cyber threat agents, thereby

setting the stage for intensifying storm patterns. If the Air Force wishes to effectively fly and fight in cyberspace, it must anticipate, assess, and prioritize cyber threat agents as well as continually act to identify and block vulnerabilities that provide opportunity to those agents. Without vulnerabilities—"flaw[s] or weakness[es] in the design or implementation of hardware, software, networks, or computer-based systems including security procedures and controls associated with the systems"—there is no threat, but the US information infrastructure is far from being free of vulnerabilities.[44]

Technology gives users tremendous opportunities, access, and efficiency; it also provides attractive capabilities to various threat agents who intend to harm users, society, the economy, and the country. Vulnerabilities are easy to exploit from anywhere across the globe. The US information infrastructure has become so intertwined among government, business, health, and personal users that all entities using the infrastructure are vulnerable. Achieving a cyber domain totally free from vulnerabilities is simply not possible, given the constant evolution of technology and growing sophistication of cyber threat agents. In view of the persistent nature of vulnerabilities in the cyber domain, users and agencies at all levels must remain vigilant.

A significant step toward increased vigilance came in 1999 when the MITRE Corporation published the first official dictionary that defined terms used to discuss the vulnerabilities of computer systems. Terming the naming standard for information-security vulnerability "common vulnerabilities and exposures" (CVE), MITRE defined universal vulnerability as a state in a computing system (or set of systems) that allows an attacker to execute commands as another user, access data contrary to the specified access restrictions for that data, pose as another entity, or conduct a denial of service.[45] In addition to defining common terminology for vulnerabilities, MITRE defined the term *exposure* as a state in a computing system (or set of systems) that, though not a universal vulnerability, either (1) allows an attacker to conduct information-gathering activities or (2) allows an attacker to hide activities, including a capability that behaves as expected but can be easily compromised.[46] Today, the CVE is sponsored by the National Cyber Security Division at the DHS, whose objective remains providing one common language as a bridge between information tools and services. In 1999 the CVE listed 663 security

issues; as of 1 November 2006, the CVE dictionary contained 20,074 unique information-security issues.[47]

In combination with the CVE national vulnerability-naming standard, the National Institute of Standards and Technology maintains a national, comprehensive vulnerability database sponsored by the DHS's Cyber Security Division / US Computer Emergency Readiness Team that combines all publicly available US government vulnerability resources and provides references to industry resources.[48] A quick search for statistics regarding vulnerabilities from 1988 to 2006 revealed a staggering increase from two to nearly 6,000.[49] As vulnerabilities skyrocketed in the last several years, the attack sophistication, technical knowledge, and availability of malicious tools have also proliferated. Researchers at the Software Engineering Institute at Carnegie Mellon University prepared a briefing in 2002 titled "Cyberterrorism" to characterize these trends (fig. 3).

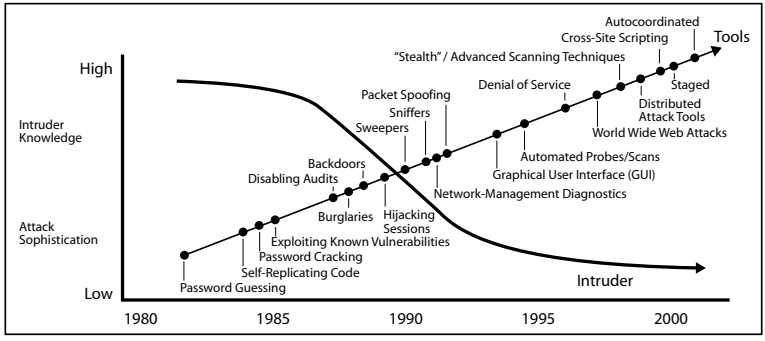


Figure 3. Attack sophistication versus technical knowledge of intruders. (Adapted from Howard F. Lipson, "Building Survivable Systems from COTS Components: A Risk Management Approach" [Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2002], 6, http://www.iccbss.org/2002/pdf/February%204/Panel/Lipson_Howard-surviv%20panel.pdf.)

The convergence of existing threat agents, vulnerabilities, attack sophistication, and technical knowledge of intruders is creating conditions for a remarkable storm. The thunderclouds are forming. The Air Force not only must create a road map that anticipates, assesses, and prioritizes cyber threat agents but also must continually act to identify and mitigate vulnerabilities. Further, it must chart how it will fall

in with the way ahead for US national strategy and existing cyberspace efforts of the DOD.

Battling the Simultaneously Challenging Winds of Change: The Way Ahead for US National Strategy

> *The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible.*
>
> —Pres. George W. Bush
> *National Strategy to Secure Cyberspace*

Forecasting the weather, although based on empirical and statistical techniques, is difficult due to the sometimes unpredictable and often changing atmospheric conditions. In much the same way, as the US government tackles the challenge of mitigating risk in the cyber domain, conditions and circumstances constantly and rapidly evolve. Even so, the government continues to pursue ways to secure cyberspace so that threat agents cannot jeopardize national security.

National Strategy. The US national policy concerning cyberspace security is clear, as is the strategic way ahead. The challenge for governmental departments lies in implementing and operationalizing the national strategy. The Air Force must define roles and missions in cyberspace consistent with the national strategy.

In February 2003, the president released the *National Strategy to Secure Cyberspace*, which outlined five priorities for national cyberspace security:

1. A national cyberspace-security response system
2. A national cyberspace-security threat- and vulnerability-reduction program

3. A national cyberspace-security awareness and training program
4. A means of securing government's cyberspace
5. Cooperation between national security and international cyberspace security

The strategy also outlined explicit actions required of federal agencies, including the DOD and the Department of the Air Force. Specifically, the strategy requires federal agencies to

1. continuously assess threats and vulnerabilities to federal cyber systems,
2. identify and document enterprise architectures,
3. continuously assess threats and vulnerabilities,
4. implement security controls and remediation efforts,
5. authenticate and maintain authorization for users of federal systems,
6. secure federal wireless local area networks,
7. improve security in government outsourcing and procurement, and
8. develop specific criteria for independent security reviews as well as reviewers and certification.

The national strategy goes on to highlight that the foundation for the government's cyber security requires assigning clear and unambiguous authority and responsibility for security, holding officials accountable, and integrating those requirements into budget and capital-planning processes.[50]

As part of the accountability process, Congress passed the Federal Information Security Management Act (FISMA) as part of the Homeland Security Act of 2002 and the E-Government Act of 2002. This act requires government agencies to secure the information and information systems that support their operations and assets, including those provided or managed by another agency, contractor, or other source.[51] It further requires agencies' chief information officers and inspectors general to report results of annual reviews to the Office of Management and Budget for execution of oversight responsibilities and to draft an annual report on agency compliance to Congress.

Government Report Card. The FISMA legislation aimed to develop a comprehensive framework to protect the government's information, operations, and assets. In the most recent report of the Office of Management and Budget to Congress (1 March 2006), the DOD scored among the lowest of the 24 government agencies or departments required to comply with FISMA. Based on reports of the chief information officer and inspector general, the Office of Management and Budget found that the DOD did not have an effective plan of action or milestones to address deficiencies in information-security policies, procedures, and practices.[52] It also characterized the DOD process of certification and accreditation as poor. Finally, the Office of Management and Budget noted the DOD's inclusion in the lowest percentage category (0–50 percent) for completing system inventory. As a result, the Congressional Committee on Government Reform gave the DOD an overall F on its computer-security report card for 2005, lowering the grade from the previous two years' Ds (table 8).

Table 8. Federal computer-security report card, 16 February 2006

Government-wide Grade: D+			
	2003	2004	2005
Department of Defense	D	D	F

Although the federal government's report card for computer security is less than flattering, there exist significant reports and initiatives in place that map out the way ahead from a national strategic level. The President's Information Technology Advisory Committee published *Cyber Security: A Crisis of Prioritization* in February 2005, and the National Science and Technology Council released the *Federal Plan for Cyber Security and Information Assurance Research and Development* in April 2006. In addition to these documents, the DHS published *Cybersecurity for the Homeland* in December 2004, and the GAO published *Critical Infrastructure Protection: DHS Faces Challenges in Fulfilling Cybersecurity Roles* in May 2005 and *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* in September 2006. Each of these documents is an excellent resource for learning more about cyberspace and its inherent weaknesses and vulnerabilities. More importantly,

these reports highlight several findings and recommendations that must be addressed. Table 9 summarizes some of the key findings and recommendations that the reports have in common. As the federal government attempts to mitigate risk in the cyber domain, the key components for success include assessment, integration, investment, coordination, and partnerships—no one agency can conquer this challenge alone.

The Air Force and the Cyber Domain. Again, when Air Force leadership revised the service's mission statement to say "fly and fight in air, space, and *cyberspace*," it acknowledged the importance of the cyber domain and recognized that success in future conflicts would require focusing on multiple domains. Before the Air Force can effectively lead in the cyber domain, however, it must first fully understand the current US cyber situation. The service must examine current cyber conditions, analyze cyber threats, dissect current vulnerabilities, and clearly define how and where it can contribute to the national cyberspace strategy. Once the Air Force fulfills these tasks, it can then focus on the nature of war in the cyber domain and consider the implications for military doctrine. This kind of shift in focus will require a new kind of thinking. As President Lincoln said in 1862, "The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew."[53]

The Cyberspace Domain of War

> *Although attacks in the cybersphere do not involve use of physical weapons, their destructive impacts, physical and otherwise, may be no less lethal to societies.*
>
> —Jeffrey R. Cooper
> "Another View of Information Warfare"

For more than a decade, volumes of scholarly works have contemplated the implications that the information age has for national security, warfare, and military strategy. Nearly all of them concluded that the explosion in variety, volume, and velocity of information and associated technologies has birthed a profoundly new environment with dramatic implications for

Table 9. Findings and recommendations of reports

Findings and Recommendations	*Cybersecurity for the Homeland*	*Critical Infrastructure Protection: DHS Faces Challenges in Fulfilling Cybersecurity Roles*	*Federal Plan for Cyber Security and Information Assurance Research and Development*	*Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*
Coordinate with private sector	X	X	X	X
Conduct threat/risk assessments	X	X	X	X
Improve integration with other agencies	X	X	X	X
Improve outreach/ coordination	X	X	X	X
Increase investments in research and development	X	X	X	X
Develop metrics	X	X	X	X
Improve information sharing	X	X	X	X
Develop public/private partnerships	X	X	X	X

Source: Data compiled from the documents cited.

military operating concepts as well as new methods of fighting that broaden the span of effects across the spectrum of war.[54] Nearly all strategic thought also concludes that the nature of war itself in this new environment remains fundamentally unchanged and will likely remain so in the foreseeable future.

Emergence of the "information environment" and concepts of network-centric warfare resulted directly from harnessing the opportunities of cyberspace as a new domain. The conduct and character of war are indeed in the throes of sweeping change, enabled largely by new capabilities provided by cyberspace. Evolutionary and revolutionary changes in war fighting result from the emergence, integration, and synergies of new content and noncontent cyber activities. We therefore require new military operating concepts.

The Air Force policy directive on concept development directs that new operating concepts consider the nature and theory of war as well as the "American Way of War"—a characterization of war fighting that emphasizes American approaches to war—in their formulation.[55] Accordingly, the following section reviews the nature and conduct of war inclusive of the cyberspace domain and its effects on operating concepts. It also reviews the role of cyberspace and new cyber operating concepts in military operational design, the joint functions of war, and the principles of war.

Conduct of War in Cyberspace

The phrase "nature of war" describes the fundamental qualities of war. We use the two bedrock theories on the nature of war—Carl von Clausewitz's *On War* and Sun Tzu's *The Art of War*—to consider new military operating concepts.[56] We also consider new cyber operating concepts in view of the American Way of War.

The Classics. Clausewitzian war is a violent, human endeavor undertaken to achieve political objectives and seek the enemy's submission to one's will; it is executed with an uncertain, probabilistic outcome. For Clausewitz, information and intelligence had limited value in overcoming the fundamental uncertainty of war.[57] Because one envisions war fighting in cyberspace primarily as a nonkinetic, information-based approach, the concept of war in this domain as a Clausewitzian conflict is indirect but still highly rele-

vant. At all levels of war, cyber weapons target leadership by compressing, confusing, and complicating the decision cycle. Cyber weapons can therefore obfuscate the employment and focus of traditional military capabilities, the accomplishment of military operational objectives, and, ultimately, the will to fight. At a more strategic level, Clausewitz is instructional in his recognition that information (as intelligence) will not likely yield complete and accurate situational awareness due to the interplay of knowledge and deception, coupled with the instantaneous temporal conditions established by the activities of data and information flow in cyberspace.[58]

According to Sun Tzu, information determines success or failure in war. He held that complete knowledge of enemy and self is attainable, therefore enabling selection of the correct strategy for success in battle—perhaps even producing victory without battle.[59] For Sun Tzu, violence comprises only a part of war—and engagement is a last resort—after one has failed to convince the adversary to capitulate either through demonstrated ability to win the battle or deception that demonstrates the same. Cyberspace directly enables the information-based war envisioned in Sun Tzu's theories, immediately capturing the concept of achieving information advantage and applying it to execute and win wars.

The American Way of War. The conduct of war in cyberspace plays to American strengths: controlling tempo and initiative through rapid global reach and agility, neutralizing the adversary's C2 capabilities, applying deadly force with minimal collateral damage through precision strike, and minimizing exposure of forces through standoff engagement and rapid establishment of air supremacy, all underpinned by advanced-technology solutions.[60] Operating in cyberspace is a global activity that provides a broad span of effects, ranging from benign presence through precision strike, by employing nonkinetic solutions and facilitating kinetic effects increasingly unconstrained by time and distance. American forces directly enabled the "shock and awe" strategy that delivered overwhelming military effects in Iraq by integrating nonkinetic cyber capabilities with traditional force-application approaches.

Military Operational Design

Elements of operational design include effects, objectives, and termination; the set of desired effects achieved through

tactical actions represents the conditions needed to achieve end-state objectives for termination.[61] The generalized set of effects sought by cyber weapons (knowledge of the adversary's presence in and use of cyberspace, assurance of friendly systems and the ability to operate in and shape cyberspace, and military operational advantage in cyberspace) includes the informational conditions necessary for achieving the military's strategic objectives in cyberspace. Both directly and indirectly, cyber ISR, attack, and defense capabilities are applied (tasks) to achieve such effects.

Operating concepts and missions have yet to fully employ and realize the tremendous capabilities offered by net-centric warfare, and, certainly, the range of effects provided by cyber capabilities in a net-centric environment has yet to be observed in a showdown force-on-force, peer-competitor environment. We have isolated only largely unintegrated examples and hints, and our own progress in developing organizations, processes, and tools for a grand information strategy is nascent. However, the information-based activities resident in the cyber domain are undoubtedly growing in significance, both relative to other war-fighting domains and as a distinct class of war-fighting capabilities.

Without robust empirical evidence, predicting the impact of operating in this domain, perceiving whether the nature of war itself will change as a result, and successfully executing the task of planning future forces and capabilities carry a degree of uncertainty and risk. Wedded to traditions of a high state of readiness and overwhelming force capabilities to maximize sovereign options and freedom of action, the American Way of War finds itself increasingly challenged by cyberspace-enabled conditions because of its tendency to underemphasize alternative belief systems, culture, and revolution. These too are enabled by cyberspace and are set in a global context. Consequently, the American Way of War must continue to evolve to ensure relevance not only for wars that play to American military strengths but also for those that evermore creatively employ the opportunities of cyberspace.

The Role of Technology. Although one finds widespread agreement that technology developments remain fundamental to enabling new ways of operating in cyberspace, expert views diverge on whether technology drives new operating concepts or whether new concepts flow from the creative ap-

plication of technology. The difference has significant implications for war fighting: the former rewards investment in ever-more advanced technology, while the latter rewards ingenuity in applying tools in new ways that can overcome technological superiority. Under the right conditions, either approach can provide a relative or niche advantage in information. Furthermore, a small number of scholars believe that the near-infinite possibilities implied by the latter are so profound that they may eventually result in fundamental change to the nature of war.

The wide range of expert views on the impact of the information revolution in warfare demonstrates a significant degree of uncertainty in understanding the longer-term effects of cyber capabilities. For example, Lonsdale found that technological developments associated with the information revolution could have significant geopolitical and strategic impacts, but he believed that such developments would not drive information to predominate as an element of national power.[62] Similarly, Douglas Dearth and Charles Williamson found that ends and means of war will change in the information age.[63] Jeffrey Cooper and Daniel Goure offered that technology fundamentally changed the way military forces are managed, integrated, and commanded in warfare but that war-fighting strategy itself had not changed. Cooper also determined that new, nongovernmental entities would likely emerge as fundamental elements of the national security structure.[64]

Moving toward the opposite end of the spectrum, Michael Brown observed that new synergies in force application introduced through advances in information technology do have the potential to revolutionize warfare but that, ultimately, technological advantage itself would not guarantee success in war.[65] Michael Vlahos commented that emerging technology would enable, but not be the driver for, a fundamentally new social order characterized by revolutionary war—a type that America is both incapable of foreseeing and unable to control because of its great-power status.[66] David Alberts found that "information technology not only will change the nature of what we know today as war . . . but will also spawn a new set of activities that will become familiar to future generations as constituting 'warfare.'"[67] The uncertainty carried by new cyber capabilities introduces risk for selecting new war-fighting

strategies and making related investments in cyber resources. We need a common approach to evaluating and characterizing the changes and effects of operating in cyberspace; such an approach would greatly facilitate resource investments and the formulation of new concepts of operating in cyberspace.

Principles and Functions of War. Joint Publication 3-0, *Joint Operations*, lists land, air, sea, and space as war-fighting domains but does not specifically designate cyberspace as such. Rather, it identifies cyberspace (i.e., the EM spectrum) as a physical factor of the operational environment that aggregates people, organizations, and systems as actors on information in the physical, cognitive, and informational dimensions.[68] As such, joint doctrine provides a model that can describe the aggregate role of information in military operations but underemphasizes the requirement to manage and fight EM spectrum-level activity. At the same time, doctrine identifies four of the six joint functions—C2, intelligence, fires, and protection—as directly supported by cyber capabilities.

A revision to joint doctrine in 2006 expanded the traditional nine principles of war to include three new principles. Derived from what was formerly referred to as "military operations other than war," these include restraint, perseverance, and legitimacy, reflecting a broader military role across the spectrum of peace and conflict and including specifically the missions of homeland security, stability operations, and flexible deterrent options.[69] This change also recognizes the growing prevalence of military operations outside major combat scenarios as well as the influence of globalization and its enablers in shaping the types of conflict in which the United States engages. Activities in cyberspace related to these nontraditional operations not only potentially amplify presence but also add a broad array of tactical capabilities to these types of fights. Operating in cyberspace at the data level to support and execute these functions offers tremendous opportunities as well as risk.

The principles of war are supported through the application of cyber capabilities both directly and as enablers. Table 10 demonstrates each of the principles by providing a mapping of the potential application of cyber roles and capabilities. The following section, "Operating in Cyberspace," describes specific cyber capabilities.

Table 10. Principles of war and cyber capabilities

Notional Military Operation				
Principle	*Purpose*	*Objectives*	*Primary Cyber Role*	*Sample Cyber-Capability Application*
Objective	Attain political goals	Destroy enemy-force capability	Offensive	Cyber ISR for intelligence preparation of the operational environment (IPOE), cyber attack to control or disable enemy systems
Offensive	Achieve military objective	Seize, retain, and exploit initiative	Offensive	Cyber ISR for IPOE, cyber attack to control or disable enemy systems
Mass	Produce decisive results	Concentrate combat power at right time/ place	Defensive	Protect and enable C2 / command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks through layered defense, self-healing, and robust reconfiguration
Economy of force	Preserve capability to mass	Enable secondary missions	Defensive	Provide stand-alone, nonkinetic options
Maneuver	Preserve freedom of action	Secure positional advantage of forces	Defensive, enabling	Cyber ISR for IPOE, cyber attack to control or disable enemy systems
Unity of command	Ensure unity of effort	Enable application of forces to common purpose	Defensive, enabling	Protect and enable operability of C2/C4ISR networks through layered defense, self-healing, and robust reconfiguration
Security	Enhance freedom of action	Reduce friendly vulnerability to hostile acts, influence, and surprise	Defensive	Cyber defense and cyber ISR
Surprise	Gain combat power advantage	Support rapid decision making, deception, and operations security	Offensive	Provide assured operations of systems, cyber attack to support MILDEC
Simplicity	Succeed in operations	Enable planning and execution	Enabling	Provide assured operations of systems
Restraint	Limit collateral damage	Prevent unnecessary use of force	Offensive	Provide stand-alone, nonkinetic options
Perseverance	Ensure commitment	Attain national strategic end state	Enabling	Provide assured operations of systems
Legitimacy	Maintain will to fight	Attain national strategic end state	Enabling	Provide assured operations of systems

Operating in Cyberspace

I felt that on the first night, the power should have gone off, and major bridges around Belgrade should have gone into the Danube, and the water should be cut off so that the next morning the leading citizens of Belgrade would have got up and asked, "Why are we doing this?" and asked Milosevic the same question.

—Lt Gen Michael Short
Combined Force Air Component Commander
Operation Allied Force

If they want to fight with us in cyberspace, we're willing to take them on there, too.

—Lt Gen Robert J. Elder Jr.
Commander, Eighth Air Force
Commander, Air Force Cyber Command

Air Force cyberspace operations consist of the integrated planning, employment, and assessment of military capabilities to achieve desired effects in cyberspace in support of the combatant commander's objectives. Cyberspace operations become possible only with appropriately trained personnel as well as hardware and software tools that offer a mix of capabilities; cyberspace battle management, including set rules of engagement for distributed operations; measures of effectiveness; and sufficient time to employ specialized ISR functions. Cyberspace in this context includes any devices that are assigned Internet protocol (IP) addresses and that comprise the global grid, such as internetwork-connected computers, supervisory control and data-acquisition systems, the Joint Tactical Radio System as well as other IP-based radio systems, and other IP-based devices. Cyberspace capabilities must be fully coordinated with capabilities offered in other war-fighting domains.[70]

Intrinsic Characteristics as a Unique Combat Domain

Cyberspace has several characteristics that make it a unique combat domain. Time (i.e., decision cycles) is more compressed than the fastest-moving kinetic capabilities. Viruses and system break-ins come at such high pace and

speed that friendly cyber defense forces have only seconds to respond. The Internet's reach renders physical distance largely irrelevant. Operations in cyberspace have the advantage that combatants' lives are generally not at risk. At the same time, however, critical services upon which modern societies depend remain vulnerable to attack via hacking. In terms of its relevance to war fighting, these characteristics allow friendly forces a broader and more controllable span of effects, truly surgical precision, great stealth, low probability of detection, and a level of nonattribution not possible in other domains. Most importantly, these effects are not subject to the same sorts of international political consequences as are many traditional capabilities that have the same effects, such nuclear weapons.

Broader Span of Effects. Cyberspace offers the potential for nearly imperceptible system effects all the way through massive electronic means of mass destruction.[71] As networked computer chips reach deeper into the devices that we use in daily life, the capability to make minute changes in these systems offers the possibility of manipulating the perceptions of those they serve. For example, these capabilities could be used to block communications to a terrorist leader at a critical moment in his operations, causing disarray, failure of the imminent attack, and fomentation of mistrust and division amongst his supporters under the right conditions. As mentioned in the previous paragraph, one of the strengths of the cyber realm is the ability to achieve effects identical to some kinetically generated effects without the international political and legal pitfalls.

Surgical Precision. As illustrated in the previous paragraph, the cyber realm brings new meaning to the term *precision*. The precision inherent in cyber attacks goes far beyond the ability to address specific targets; the cyber realm is capable of imposing effects upon certain characteristics or parts of targets. Everything from cutting off communications to feeding bad timing or location information to an adversary can manipulate the outcome of his operations and bring real tactical, operational, and even strategic advantage to friendly forces. Depending on the circumstances, cyber capabilities could be used to produce effects such as delaying or even stopping an invasion by remotely immobilizing the lead tanks

of a force on a bridge, thus thwarting the passage of other forces.

Stealth / Low Probability of Detection. Low probability of detection and stealth are necessary conditions for effective operations in cyberspace. Both are particularly essential to conduct covert cyber ISR; cyber attack also requires a high level of access to adversary networks throughout all phases of conflict. Although cyber activities are characteristically stealthy and difficult to detect, one must still take care to prevent their discovery, which risks loss of target access, adversary knowledge of cyber capabilities readily countered or not easily replicated, and limitations of capabilities. Research should focus on reducing the requirement for stealth so that cyber can provide better deterrent effects.

Nonattribution/Untraceability. The difficulty of detecting an adversary's cyber activities also makes them more challenging to trace and attribute. Embedded in some tools and methods, these capabilities frequently require manual actions such as log manipulations. Such characteristics prove invaluable to national security because they reduce the likelihood of counterattacks and preserve military options far below the level of war. As mentioned previously in this section, they also reduce the likelihood of negative international legal and political effects when one employs cyber capabilities. In this way, one can also use them to aid other elements of national power rather than hinder them.

Cyber Capabilities

Cyberspace capabilities fall into three major categories, including cyber ISR, cyber defense, and cyber attack. Though operations in the cyberspace domain are fairly new, *Joint Vision 2020* recognized for the first time that many of the capabilities offered in this nonkinetic domain have analogs in the kinetic domain.[72] However, because operations in the cyberspace domain are virtual, the relative precedence of these capabilities is entirely different. For example, one places a greater premium on stealth and low probability of detection than one does in many kinetic operations because activities in the cyber domain depend upon continued access to target systems; detection could result in loss of access due to disconnection or improved security mea-

sures. Conversely, in the physical domains, some ISR activities, such as mapping enemy territory, can be carried out openly.

Cyber Intelligence, Surveillance, and Reconnaissance

Cyber ISR (termed computer-network exploitation in joint doctrine) is the cyber equivalent of kinetic IPOE.[73] Successful cyber attacks and defenses require the comprehensive knowledge of one's own capabilities and system configurations as well as those of an adversary's systems and their configurations, provided by cyber ISR.

As mentioned above, cyberspace operations of all types depend heavily on sufficient information on the function, configuration, and criticality of an adversary's systems. The major functions of cyber ISR involve the following general steps (see also fig. 4):

1. Potential target systems are identified through all-source intelligence, data specifically collected to access the target, and "social engineering"—the process of obtaining information on systems from people inside the organization.[74]

2. Access is obtained through direct penetration of the adversary network or through installation of trapdoors, backdoors, and multirole, customizable mobile code called cyber craft.

3. Data on the target-system configuration is then exfiltrated.

4. Analysis of the data is conducted.

5. Ultimately, a model of the adversary's target system is created.[75]

This cycle is repeated continuously to improve the target-system model and maintain its accuracy as the adversary's system administrators make changes to it.

The goal is the accurate modeling of an adversary's systems by systematically and methodically mapping his security posture in four critical areas:

1. Internet—includes external domain name, network blocks, system architecture and access-control measures, any intrusion-detection or protection devices, IP addresses of major systems and the services they are running, and enumeration of information about users and other systems.
2. Intranet—includes the same information listed above but for the adversary's internal network.
3. Remote access—includes remote-user and administrator capabilities such as dial-in phone numbers; authentication schemes and systems; virtual, private networking protocols; and remote-system types.
4. Extranet—includes connection origination, destination, type, and related access-control information.[76]

Cyber ISR is as critically important to cyber defense and attack operations as traditional ISR is to kinetic target selection in bombing or detection of a nuclear missile launch in

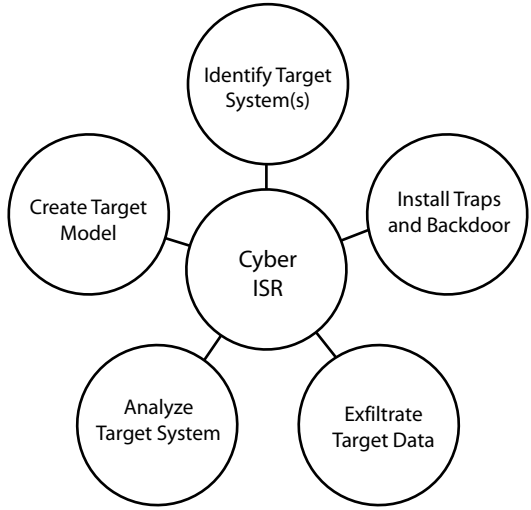


Figure 4. Principal elements of cyber ISR. (From Col William B. Sparks, "67 Network Warfare Wing Mission Brief" [lecture, Air Intelligence Agency, Kelly AFB, TX, 12 September 2006.])

national missile defense. Regardless of the war-fighting domains considered, one must spend significant time and careful effort in advanced planning and equipping for operations.

The borderless nature of cyberspace and the requirement to conduct adequate cyber ISR covertly and without attribution raise some issues for its conduct. These capabilities face legal challenges such as the separation of Title 10 (military) and Title 50 (civilian law enforcement) responsibilities to protect civil liberties, the need for a presidential finding before operations can begin, and regular reports to congressional intelligence-oversight committees.[77] Failure to resolve these restrictions will hamper cyberspace operations.

Identifying and Profiling of Target Systems. Identifying and profiling represent efforts to collect preliminary data as a starting point to gain sufficient knowledge about a target organization. Friendly forces can then use this information to understand how the adversary might configure his systems. One must make a determination of the type (defensive or offensive) and intended scope of a particular cyberspace operation based on the desired effects prior to identifying the target and beginning cyber ISR in support of it. Only after one fully understands the desired effects should identification of target systems begin. Existing all-source intelligence contains a wealth of information about potential adversaries that could be leveraged. Intelligence-gathering efforts on new targets should be properly authorized, submitted, and prioritized for collection as needed, including social-engineering activities involving human intelligence.[78] Types of information typically collected at this point include the adversary's organizational structure, publicly available personnel data, data archived on search engines, network-security-related policy documents, information from former and disgruntled employees, Internet-connectivity link providers, and public-access Web pages as well as other access sites. One can obtain registration information concerning Internet domain names and IP addresses from central Internet registration authorities such as the Internet Corporation for Assigned Names and Numbers or subordinate regional registries.[79]

After collection of the needed general information about the target, a more technical effort should begin. Tracking

the sending and receiving addresses used by the target's systems permits accurate profiling of network traffic.[80] In turn, profiling allows identification of the network protocols used and the addresses of machines performing certain functions on the target network, giving clues about its topology. One needs reliable identification and profiling of the target as a starting point to perform the next step: scanning, access, privilege elevation, and installation of persistent presence.

Access and Installation of a Persistent Presence. Regardless of whether one uses social engineering, interception, or more direct methods, one must gain unauthorized access to an adversary's systems in order to conduct effective operations. The goals of this stage include mapping all possible avenues to approach the target, access the target and elevate privileges to administrator level, and, finally, install the necessary software to maintain continual access and control. To determine which "doors" have been left open to the outside world, one should remotely and discreetly sweep and scan candidate systems, using active, passive, and fully automated techniques designed to determine the operating systems and services available via access points also known as ports.

Once these available ports and services become fully known, the next task entails determining which of these offers the possibility of basic access—a process called enumeration.[81] One can use an ever-expanding variety of methods to effect enumeration and determine the operating systems, applications, and network protocols yet remain anonymous and undetected:

1. Cracking or exploiting passwords
2. Exploiting known hardware and software vulnerabilities
3. Exploiting network-protocol flaws
4. Examining operating system, program source code, and executable files for new security flaws
5. Compromising Web servers
6. Installing sniffer programs

7. Installing or registering known backdoors (e.g., rootkits), trapdoors, and custom cyber craft designed to collect information
8. Proliferating worms, viruses, and other mobile code designed to grant access[82]

Since anonymity and deniability are essential elements of cyber operations, one employs methods such as network-address spoofing during this phase.[83] One should also take care to ensure that the intensity of operations (network traffic) does not rise to a level that would allow easy detection through the use of slow scanning and judicious use of other tools and techniques.

Mapping of Enemy Systems and Data. After obtaining continual access and administrative control, cyber ISR focuses on using these new capabilities to gather complete information about the configuration of the adversary's systems. Known as pilfering in hacking circles, the mass exportation of system data from adversary hosts essentially amounts to using all accessible data to assemble a map of the adversary's systems.[84] It represents the final stage of technical data gathering necessary before analysis can begin. Exfiltrating password "hashes" or password files, further password cracking, and reading cached logon information are important methods of expanding privileges and pilfering critical system files that contain data on every user and server needed to assemble a system map.

Another method of exfiltration involves the use of remote applications that can operate through backdoors installed during earlier access attempts. Remote control of machines on the adversary's network offers access to a wealth of system information, particularly when coupled with elevated system-administrator privileges.[85] One can implement remote-control capabilities on a compromised system to divert transmissions of traffic from normal paths (ports) that are blocked to paths left open for routine traffic. This process of port redirection is typically used to circumvent network-security devices such as firewalls.[86]

After obtaining large amounts of data and control over adversary Internet, intranet, extranet, and remote-access network and computing resources, one can complete

the mapping process. A completed map should include information about both the internal and external systems that comprise the adversary's network. A basic version would include administrative account names and passwords, names and addresses of servers and the network ports and protocols they use to provide services, a map of the data housed in application servers, a logical map of the interconnection of network-switching devices, firewall and other security-device configurations, and documentation on network remote-access services. More advanced maps should correlate vulnerabilities in different versions of operating systems, application-software programs, and the hardware's firmware versions. A comprehensive map greatly improves the likelihood of accurately determining an adversary's capabilities and intent.

Analyzing an Adversary's Capabilities. A solid, technical map of how the adversary's cyber systems function is not sufficient to fully understand his capabilities, however. Although the part played by some systems, such as firewalls, in the overall scheme of an adversary network is obvious, some are so generic that their purpose remains unclear. They may even serve many purposes simultaneously or at different times, depending on the software loaded and the hardware attached or embedded. One should conduct further traffic monitoring to determine their typical primary and ancillary functions.

Depending upon the extent to which an adversary's system administrators monitor the target internal network, it may even be possible to employ system scanning and mapping applications to determine the actual functions and uses of various devices on the network. Generally, however, this is a manual process because one can characterize many actions as defensive, offensive, or simply routine maintenance. Final characterization of capabilities requires the attention of fully trained experts in network infrastructure and application programs, schooled in network defense and offense. Taken together, profiled traffic and an adversary's system maintenance and defense—even attack exercises and methods—reveal the full gamut of capabilities.

Determining an Adversary's Intentions. Determining intentions can prove extremely difficult even after one fully knows the adversary's technical capabilities and has documented his behavior. However, the existence of target-network servers and other devices dedicated for use in actual offensive operations or exercises, connections to external networks with disparate IP address sets, or observed pilfering of data from other networks serve as important indicators of offensive intent. One can obtain other indicators through an exhaustive search of materials exfiltrated from the target network. Specific evidence of intent includes coordination procedures for offensive operations, actual targeting plans or lists, administrator chat sessions that discuss such events, and manuals for executing attacks. All of these factors are important in determining the adversary's defensive or offensive intent, but they are even more important as indications and warnings of impending attack.

Planning Attacks / Retaliatory Strikes. Cyber ISR is essential to successful prosecution of any cyber attack or defensive retaliatory strike. Earlier parts of this section thoroughly outlined the extensive research and analysis required. One should not undertake offensive or retaliatory actions before conducting adequate cyber ISR and obtaining proper authorization to perform attacks.[87] In the interim and because of the breadth and depth of analysis required, it may be necessary to perform an array of defensive measures until one can make and execute adequate preparations for offensive operations.

Cyber Defense

Communications are an essential element of every aspect of Western society, affecting the functions of every element of national power, including military power. Defense of those capabilities is critical to the national survival of societies and nations. Cyber defense consists of the protection, detection, and attribution of computer-network attacks as well as the reconstitution and recovery of friendly information systems after an attack from an adversary's attempts to destroy, disrupt, corrupt, or usurp

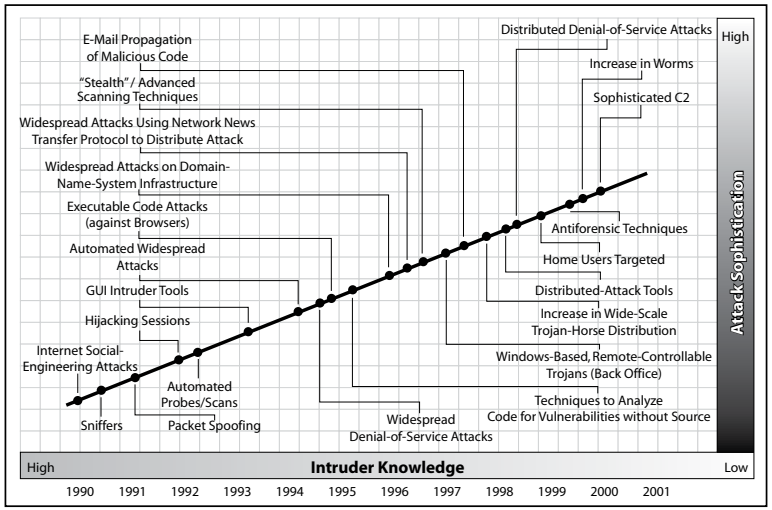


Figure 5. Trends in cyber attack. (From "Incident and Vulnerability Trends, 2003" [Pittsburgh, PA: Carnegie Mellon Computer Emergency Readiness Team Coordination Center, 2003], 18.)

them.[88] Attacks on our national and military information infrastructure are multidimensional, constantly increasing in frequency and scope. Due to the open distribution of automated tools for hacking on the Internet, the expertise required to execute increasingly sophisticated attacks has declined significantly (fig. 5). Friendly forces must employ coordinated, defense-in-depth capabilities to anticipate and preempt attacks on our information systems.[89] When an adversary successfully attacks computers and networks, information defense must rapidly minimize their effects and develop courses of action to respond and prevent a recurrence.

Friendly cyber defense will anticipate and defeat a wide array of persistent and simultaneous attacks. In addition to defending against other nation-states, cyber defense must guard against irregular network threats from such entities as terrorists; drug cartels; all types of hackers, regardless of intent; as well as accidental "insider" events and intentional attacks from disgruntled employees. The DOD and

the Air Force have adopted a defense-in-depth strategy in order to meet these challenges.

Defense in depth consists of several control measures involving personnel, technology, and operations. Personnel-related measures include administrator-training standards, user-awareness training, and security procedures for personnel, physical, and system-security administration. Aside from the actual technological systems employed, methods of employing the systems to protect networks include layering, risk assessments, acquisition and security criteria, as well as certification and accreditation of new systems. Assessment includes both "gray" (cooperative) and "red" (covert) system tests by friendly security experts.[90] For example, Operation Eligible Receiver, a "red hat" exercise, was conducted in 1997 and 2003 to assess the DOD's system vulnerabilities through actual hacking and scanning.[91] The DOD concept of defense in depth involves protection at four layers: network and infrastructure, enclave boundaries, computing environment, and supporting infrastructures such as certificate-registration authorities. In operations, implementation of defense in depth requires assessments, monitoring, intrusion detection and warning, as well as response to attack and reconstitution in the event of a successful attack.[92]

Protection from Attack. Indications and warnings derived from properly conducted cyber ISR afford the best protection against adversary attacks. Firewalls and router-access control measures are the principal direct means used to protect networks from attack. One can employ other methods, however, to improve the robustness of these basic structures—for example, redirecting attacks via packet forwarding or attracting hackers to artificially created environments ("honeynets") where they can be effectively monitored, controlled, and identified without their knowledge.[93]

Attack Detection and Attribution. Attacks can come in many forms (table 11), but the Air Force employs standard intrusion-detection systems at every echelon of networking to ensure the detection of attacks.[94] Honeynet environments and system-management "traps" that generate alarms upon performance of certain critical management actions can also aid in detection of attacks.

Table 11. Classes of attack

Attack	*Description*
Passive	Passive attacks include analyzing traffic, monitoring unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information (e.g., passwords). Passive intercept of network operations can give adversaries indications and warnings of impending actions. Passive attacks can result in disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These attacks may be mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-in	Close-in attack consists of a regular individual's attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry, open access, or both.
Insider	Insider attacks can be malicious or nonmalicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. Nonmalicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as "getting the job done."
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code, such as a backdoor, into a product to gain unauthorized access to information or a system function at a later date.

Source: Information Assurance Technical Forum, *Defense in Depth* (Washington, DC: Government Printing Office, 2002), 5.

One can also employ honeynets to attribute attacks despite attackers' attempts to hide their identities via IP spoofing. Honeynets can produce direct technical information about attackers, keeping them "on the line" long enough to be traced.[95] Efforts such as the Hacker Profiling Project at the United Nations Interregional Crime and Justice Research Institute are also developing new methods to attribute at-

tacks based on the software left behind or the methods used. Indications and warning from cyber ISR, however, remain the best and most reliable method of attribution.

Automated Attack Responses and Operator Alerts. A number of new network-protection systems are capable of detecting and providing a limited, automated protective response to attacks.[96] Linking detection to automated responses, automated operator alerts, and alarms is key to ensuring that defense remains viable as the volume of network traffic increases. One must take care to ensure that these automated responses cannot be manipulated by attackers or result in self-imposed denial-of-service attacks and adverse effects on operations.

Self-Healing of Systems and Networks. A fourth-generation networking capability, self-healing has begun to appear in commercially available systems; it is highly desirable in environments that require high-assurance computing and networks.[97] Networks have long possessed limited ability to reroute traffic as a result of link failure, and technologies such as server "clustering" have provided redundancy for many years. As these capabilities mature, they will become available in every computing device. As with the automated responses mentioned in the previous section, this capability must be high assurance; otherwise, hackers could manipulate it.

Rapid Recovery after Attack. For many years, backup systems have served as the primary element in recovery from data disaster and attack. However, fast and inexpensive storage, coupled with intrusion detection, has dramatically decreased the time required to restore a system. The promise of lightning-fast automatic attack recovery should be tempered by the same cautions facing other features of automated systems, namely the risk that the system could be manipulated by attackers or suffer a malfunction.[98]

Cyber Attack

One can use a large array of existing technical capabilities to conduct offensive operations in cyberspace against an adversary's data, systems, and networks in support of the combatant commander's objectives. In addition to certain capabilities in special technical operations already in existence, research and development constantly produce

more options. New, more flexible capabilities such as cyber craft that can serve cyber ISR, defensive, and offensive purposes are under development to ensure that our capabilities keep pace with ever-changing threats and defenses.[99]

One can also use "commercially available" attack methods as a model to augment designs for new capabilities (table 12, outlined in order of increasing sophistication required to execute them). Though not exhaustive, this list covers the major categories of attack and describes their most common methods of execution. Although one can apply the vulnerabilities they exploit and the concepts they use to enhance designs, one should not use the actual code without thorough investigation.[100] Regardless of whether commercial or government sources developed the capability, all attacks and methods of access become highly perishable once revealed.

Cyber-Attack Authorization. As mentioned earlier, all cyber activities require proper authorization prior to execution. This is particularly true of cyber attack due to its more aggressive nature. Unfortunately, under current law and given authorizations, cyber attack is so heavily restricted that it has not yet been effectively employed. Even under international law, including the Geneva Conventions and the Law of Armed Conflict, the legality of cyber capabilities has not been addressed though the concepts of discrimination and proportionality can still be assumed to apply.[101] The section "Concluding Thoughts" will explain the measures that should be taken to improve leadership confidence in these capabilities and allow for their effective employment.

Disruption of Adversary Command and Control Systems, Processes, and Data. The capability to temporarily disrupt the operation of adversary C2 systems is a key element of cyber attack. The categories of attack typically employed to disrupt systems involve exploiting vulnerabilities or malicious software.[102] System disruptions are effective for two principal reasons. First, the interruptions can be triggered to occur at a time and place of our choosing. Second, they appear to be "normal" system disruptions and are therefore covert. Their covert nature protects the access gained under cyber ISR and allows reuse as long as they are not compromised.

Denying Access to an Adversary's Systems and Data. Denying access to an adversary's systems without destroy-

Table 12. Common categories and methods of cyber attack

Attack	*Description*
Denial-of-Service Attacks	
Flooding	Sending extraneous data or replies to block a host service
Synchronize (SYN)/reset (RST) flooding	Exploiting limited cache in IP stack to block connections
Smurfing	Using the IP broadcast system and IP spoofing to multiply floods
Out of band / fragment attacks	Exploiting vulnerabilities in IP stack kernel implementations
Nuking	Using forged messages to reset active connections
Specific denial of service	Generating requests that block one specific vulnerable service
Malicious Software Attacks	
Logical bomb	Program designed to cause damage under certain conditions
Backdoor	Program feature allowing remote execution of arbitrary commands
Worm	Program that spawns and spreads copies of itself
Virus	Code that self-reproduces in existing applications
Trojan	Program-in-a-program that executes arbitrary commands
Exploiting Vulnerabilities	
Access permissions	Exploiting read/write access to system files
Brute force	Trying default or weak login/password combinations
Overflow	Writing arbitrary code behind the end of a buffer and executing it
Race condition	Exploiting temporary, insecure conditions in programs
IP Packet Manipulation	
Port spoofing	Using commonly used source ports to avoid filtering rules
Tiny fragments	Using small packets to bypass firewall protocol/port/size checks
Blind IP spoofing	Changing source IP to access password services without a password
Name-server ID "snoofing"	Blind spoofing with calculated false ID numbers name-server (NS)-caches
Sequence-number guessing	Calculating TCP sequence (SEQ)/acknowledge (ACK) numbers to spoof a trusted host
Remote-session hijacking	Using spoofing to intercept and redirect connections
Insider Attacks	
Backdoor daemons	Opening a port for further remote access
Log manipulation	Removing traces of attacks and unauthorized access
Cloaking	Replacing system files with Trojans to hide unauthorized access
Sniffing	Monitoring network data to find sensitive data (e.g., passwords)
Nonblind spoofing	Monitoring network to hijack active or make forged connections

Source: Ankit Fadia, *Network Security: A Hacker's Perspective* (Cincinnati, OH: Premier Press, 2003), 165–230.

ing them is generally far less covert than disruption. Cyber denial, as it is called, typically involves employing methods under the category of denial-of-service attacks that involve flooding the adversary network overtly.[103] While execution of these types of attacks can be controlled, network defenses will likely prevent their reapplication and result in the loss of access to the adversary's systems. Therefore, careful consideration of the benefits and costs of execution should be taken into account prior to undertaking cyber denial.

Degrading an Adversary's System Performance. Degrading an adversary's cyber capabilities is essentially a less-extreme form of cyber disruption. Making access to applications or networks slow or intermittent can effectively distract the adversary and slow his decision cycles. Unlike cyber disruption, however, an adversary's system personnel retain access to their systems and can monitor system performance in real time, potentially exposing friendly efforts at cyber degradation. If such degradation efforts are discovered, they will suffer the same consequences as found in cyber denial: loss of the ability to reuse the capability and loss of friendly access to the adversary's system.

Destruction of an Adversary's Data, Computers, and Networks. Destruction of part of an adversary's cyber capabilities has both advantages and disadvantages. Loss of the adversary's capability removes that capability from the fight and serves to coerce the adversary by demonstrating our ability and willingness to engage battle in cyberspace. Unfortunately, it also alerts the adversary to threats that his cyber capabilities face and virtually guarantees that the adversary will put more emphasis on cyber security. This, in turn, could result in a loss of friendly access to influence an adversary's networks.

Cyberspace Effects

Combatant commanders will employ Air Force cyberspace operations before, during, and after conflict in order to achieve desired effects as part of a larger joint operation. Air Force cyberspace operations will be conducted as part of a joint-force effort and with the express legal consent of the appropriate authorities. Air Force cyberspace forces will operate in accordance with the president's *National Strategy for Securing*

Cyberspace, DODD 3600.1, joint guidance found in Joint Publication 3-13, Air Force Doctrine Document (AFDD) 2-5, and legal restrictions outlined in the *DOD Information Operations Roadmap*.[104] In addition to pointing out the need to resolve doctrinal and legal issues, the *DOD Information Operations Roadmap* identifies new and novel options available only through cyberspace operations. Because cyber operations are applicable throughout all phases of a conflict, including pre- and postconflict stages, its activities can function as supported or supporting military courses of action.[105]

Cyberspace operations should be considered for use as an option of first choice through a careful consideration of potential costs and benefits. Cyber options can be particularly attractive due to the virtual elimination of risk to friendly forces and the severe reduction of adversary collateral damage and resulting reconstruction costs. When selected as a primary-effect provider, the cyber realm should be supported by other, more traditional, options, including kinetic ones. Friendly forces in cyberspace consist of software and inexpensive hardware designed to be easily reconstituted; no operators are placed at physical risk. Depending on the adversary systems targeted and the manner in which they are affected, the resulting physical damage can be controlled by the attacker. Some cyberspace options are so unique to the medium that they are not achievable by other means. Unique cyber military effects can range from paralyzing adversary command, control, and communications to execution of feints and selective or complete destruction of enemy combat systems through online manipulation by means of a variety of capabilities. In fact, some Air Force cyberspace options can allow the military to contribute more directly to the effects of nonmilitary elements of power—such as the diplomatic, informational, or economic—by holding an adversary's cyber assets at risk.

Foresight in diplomatic affairs can be a crucial advantage. Capabilities such as electronic eavesdropping to predict an adversary's initiatives, intercepting and manipulating or delaying diplomatic messages, and electronic manipulation of an adversary's intelligence can provide friendly diplomatic corps an unbeatable edge. The ability to know what the adversary will propose and what his political goals are is a strategic advantage that cannot be ignored.

The effects that cyber capabilities can bring to bear give friendly forces advantages in the informational realm and are nearly boundless. Internet-site manipulation and interception and manipulation of enemy Internet and radio-based C2 could be particularly useful in producing information effects needed to combat terrorism. In more traditional conflicts with nation-states, the cyber realm could be used to negatively affect an adversary's morale and will to continue a struggle and simultaneously buoy friendly resolve.

Economic effects could also be created through cyber capabilities. Possible effects include direct (but covert) manipulation of adversary financial markets or major industries without the negative connotations that come with sanctions, negatively affecting an adversary nation's international credit by providing false evidence of counterfeiting, and total collapse of an adversary's financial system through mass electronic transfers.

Cyber Intelligence, Surveillance, and Reconnaissance. In addition to aiding in the collection of intelligence for kinetic activities, cyber ISR used against military targets provides the capability to obtain adequate knowledge of adversary cyberspace identities, capabilities, and intentions to plan successful, friendly cyber defenses and offenses. Given the proper cyber ISR and access, nearly anything—from the isolation of adversary leaders from information and communications to the catastrophic collapse of a terrorist organization's financial network—can be accomplished. In the future, cyber capabilities will develop to the point that they can be brought to bear against adversary intelligence in ways that make it so unreliable to adversary decision makers that it affects their faith in the system and the quality of their decisions. In order to produce a more complete spectrum of effects, future capabilities must be developed to insert destructive vulnerabilities into adversary combat, intelligence, and logistics systems.

Cyber Defense. Cyber defense ensures the preservation and uninterrupted operation of friendly information systems and networks. This includes assurance that the critical aspects of data are protected, including data availability, integrity, authenticity, confidentiality, and nonrepudiation. The value of these aspects of IA to other military capabilities and elements of national power is critically high. A future capability to attribute attacks on friendly cyber forces to a specific

adversary must be developed, however, to ensure that friendly counterstrikes are properly directed. The most important potential effect of a strong cyber defense is to make cyber attack upon friendly forces seem so futile that the adversary does not even attempt it. Though cyber superiority can be obtained only in certain limited areas for only short periods of time, an aura of friendly cyber-attack invulnerability can be indispensable during the conduct of military operations.

Cyber Attack. Cyber attack can be used directly, or it can indirectly affect adversaries in a manner similar to airpower. Adversary systems can be neutralized, marginalized, destroyed, or held at risk by friendly forces in order to achieve economic, informational, diplomatic, or other military advantages, just as offensive kinetic capabilities do. Today's cyber-attack capabilities and related effects are limited by the ability to access adversary systems and by the fact that their use is apparent and easily countered. Friendly cyber forces must develop new capabilities to rapidly generate and deliver effects, irrespective of the state of adversary cyber defenses and adversary awareness of their use. A strong cyber-attack capability that could not be stopped by adversary cyber defenses would have the same deterrent effect as strategic nuclear forces. But it would also provide friendly decision makers greater freedom of action than nuclear weapons because it would not come with the same political backlash.

Recommendations on the Way Ahead

Neither a wise nor a brave man lies down on the tracks of history to wait for the train of the future to run over him.

—Dwight D. Eisenhower

The cyberspace domain is a key component in the current and future mission of the US Air Force. A thorough concept of cyberspace operations is absolutely fundamental to enable success in planning strategy, building and organizing forces, and resourcing actions required in the cyber domain of warfare. To this point, this paper has provided a synopsis of several critical factors and observations regarding the current

cyber state of affairs. Each section has put forward significant conditions and issues to provoke discussion and debate with the goal of contributing to the development of a comprehensive concept of operations for cyberspace. This section addresses these issues by advocating a holistic methodology to develop cyberspace mission capabilities for the Air Force and by highlighting essential factors contributing to the same.

Methodology

> *In bullfighting there is a term called* querencia. *The querencia is the spot in the ring to which the bull returns. Each bull has a different querencia, but as the bullfight continues, and the animal becomes more threatened, it returns more and more often to his spot. As he returns to his querencia, he becomes more predictable. And so, in the end, the matador is able to kill the bull because instead of trying something new, the bull returns to what is familiar. His comfort zone.*
>
> —Carly Fiorina
> Former Chief Executive Officer
> Hewlett-Packard

> *The concept of "Revolution in Military Affairs" is a controversial one that has been responsible for the spilling of a great deal of ink. There is widespread disagreement over how many there have been and even over a basic definition of the term. It is no doubt rather frustrating for policy-makers and practitioners to observe what might appear to be analysts debating how many RMAs can dance on the head of a pin.*
>
> —Tim Benbow
> *The Magic Bullet? Understanding the Revolution in Military Affairs*

When Air Force leadership added cyberspace to its mission statement, it recognized the changing landscape of future conflict and shifting tactics of looming adversaries. The challenge the Air Force accepted along with this recognition is to rebuff its *querencia* and to bolster its war-fighting arsenal by looking at warfare through the prism of cyberspace.

If the Air Force is to succeed in developing a capability to exploit the cyber domain to deliver sovereign options for the defense of the United States and its global interests, it must find a holistic, systematic way to gain understanding of the "how, why, who, and what" effects Air Force cyber power will have in future conflicts.

Debate over Cyberspace and the Revolution in Military Affairs. The phrase "revolution in military affairs" gained prominence after the first Gulf War and is often employed as a way to predict the future of warfare. Beginning in the early 1990s and continuing to today, the phrase is overused and often misused by those who pontificate on the subject. Most recently, the idea of the information-age RMA gained prominence. Theorists debate net-centric warfare, information technology, the rise of asymmetric threats, information warfare, and now cyberspace as potential RMAs.

Why spend any time discussing the RMA and cyber domain? The answer is simple. It is useful to argue the role of cyberspace as an RMA in order to understand the intended outcomes of adding the term to the Air Force mission statement and to frame the methodology to achieve those outcomes. According to Dr. Andrew Marshall of the DOD's Office of Net Assessment, an RMA is "a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations."[106]

When the Air Force claimed cyberspace as part of its mission, it not only acknowledged the changing terrain of conflict and the corresponding shift in tactics of would-be adversaries but also bewildered many in uniform who wondered what exactly the move implied. By changing its mission statement, the Air Force sparked much debate on the extent to which cyberspace would dominate roles, missions, and the budget. Did Air Force leadership see the addition of the cyber domain as revolutionary? If so, what did that mean?

Revolution in Military Affairs Defined. Since the early 1990s, hundreds of scholars and think tanks have published articles and entire books on the subject of the RMA, each with a slightly different slant on the definition. Some authors

went so far as to subdivide their definition of an RMA into lesser and greater RMA categories. Other scholars debate the RMA with regard to the definition of war versus warfare. Some scholars claim there have been 10 RMAs; others assert three broad periods of revolution; and still others stress specific technical innovations as revolutionary. Table 13 highlights some events that scholars consider RMAs.

Table 13. Survey of suggested RMAs

- Assyrian combined-arms tactics
- Cavalry stirrups
- Persian and Byzantine heavy cavalry
- Infantry pikes and longbows
- Gunpowder
- Cannon
- Shipborne cannon
- French military reforms of the sixteenth century
- Efficient fortress-construction methods
- Musket
- Swedish adoption of massed-volley gunfire
- British financial revolution
- Social and political upheavals of French revolution
- Introduction of corps system into armies
- Introduction of the modern staff system to armies
- Railroad, rifle, and telegraph
- Naval steam engines, metal ships, and armor
- Medical revolution
- Indirect fire and the deep battle
- Submarine warfare
- Mechanized warfare in the 1930s and 1940s
- Blitzkrieg, strategic bombing, offensive carrier aviation, and amphibious warfare
- Nuclear weapons and ballistic missiles
- People's War
- The microchip
- Cybernetics and automated troop control
- The information era

Where one draws the line for an RMA depends entirely on the restrictiveness or permissiveness of the definition used. Five of the most prominent scholarly/think-tank definitions for an RMA are listed in table 14.

While these five definitions are just the tip of the definition iceberg, there are common threads woven throughout the literature on RMAs. There is agreement that while technology

Table 14. Five prominent definitions for RMA

Definition	*Source*
An RMA involves a paradigm shift in the nature and conduct of military operations that either renders obsolete or irrelevant one or more core competencies of a dominant player, or creates one or more new core competencies in some new dimension of warfare—or both.	RAND Corporation
It is what occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase—often an order of magnitude or greater—in the combat potential and military effectiveness of armed forces.	Andrew Krepinevich
A radical change in the conduct and character of war.	Colin S. Gray
A discontinuous increase in military capability and effectiveness arising from simultaneous and mutually supportive change in technology, systems, operational methods, and military organizations.	Steven Metz and James Kievit
Refers to a step change in the basic character of warfare. An RMA should fundamentally affect strategy and the role of military power in the international system, leading to a qualitative shift in what war is and how it is conducted.	Tim Benbow

Source: Data compiled from Tim Benbow, *The Magic Bullet? Understanding the Revolution in Military Affairs* (London: Chrysalis Books Group, Brassey's Publishing, 2004).

tends to be recognized as a principal source of RMAs, it is neither necessary nor sufficient to an RMA.[107] Similarly, most scholars agree that RMAs are not accidental. They are shaped by a combination of factors that may include technology but must include organizational adaptation, war-fighting innovation, and a change in military doctrine. Given these parameters for an RMA, it is imperative that the military not overreact to each faddish trend that manifests itself; to do so would place the military in a continuous state of flux where defense priorities are endlessly shuffled.

So What? Clearly, cyberspace compared to the widely accepted definitions and historical RMAs does not yet fit the mold of an RMA. It may be a contributing factor to what is widely held as the current information revolution, but cyberspace has not caused a radical change in either the conduct or character of war. This claim is not intended to downplay the importance of the cyber domain or to say that at some future point, cyberspace will not be considered an RMA itself—or, at a minimum, a principal contributor that sparks another RMA. But, to date, cyberspace has simply added new elements to the existing game; it has not changed the game itself.[108]

Pushing aside the idea that cyberspace will revolutionize warfare allows the Air Force to shape the intended outcomes of adding the term to its mission statement and to frame a methodology to achieve those end results. If the outcomes and methodology are not identified, Air Force leadership risks making cyberspace just a cliché on par with other "commonsensical notions that have been canonized by high official blessing."[109]

Although not evident at the publishing of the new Air Force mission statement, it is now clear that the service does not regard cyberspace as an RMA but as "a domain where the Air Force conducts operations."[110] This distinction is significant. As was illustrated in the section "The Cyberspace Domain of War," cyber capabilities *support* the principles of war; they do not change them. The cyber domain is simply another place to operate. How the Air Force harnesses the power of cyberspace in support of US national interests will be determined, in large measure, by the methodology it employs to define its role in the cyber domain.

> *Exposure to new information technologies and their capabilities is potentially dangerous unless it is accompanied by changes in a number of key dimensions. Further, [there is] a recognition that the changes that are required are interrelated and hence, need to be considered in a holistic manner. They need to be coevolved.*
>
> —David Alberts
> *Information Age Transformation: Getting to a 21st Century Military*

Cyberspace Operations as a Mission-Capability Package. The methodology employed by the Air Force to define and develop its role in the cyber domain in order to deliver sovereign options for the defense of the United States and its global interests is critically important to its success or failure. Turning to a mixture of the already-known status quo will stall this effort indefinitely and potentially lead to outright failure. The Air Force must steer clear of returning to its *querencia.*

Effectively flying and fighting in cyberspace require a holistic approach designed to examine and evolve doctrine, force structure, support, research and development, and a host of other requirements to make dominance of this domain a reality. Such an approach exists within the DOD. The process is called the "mission-capability package," developed by the Command and Control Research Program (CCRP), initiated in the 1990s through a recommendation by the Defense Science Board in response to the need to better understand C2. Over the years, this organization evolved and expanded. Today, the CCRP resides under the Office of the Deputy Assistant Secretary of Defense (Networks and Information Integration) and provides out-of-the-box thinking applied to national security challenges of the information age; independent assessment and analysis of emerging issues, concepts, and approaches; and leadership for the C2 research and analysis community.[111] One of the key concepts developed by this program is the mission-capability package, aimed at developing capabilities by building institutions based on mission requirements rather than trying to satisfy mission requirements within current structures and constraints—in other words, staying away from the Air Force *querencia.* The approach developed by the CCRP to build a mission-capability package should be used by the Air Force to exploit the power of cyberspace in support of US national interests. From this model, the Air Force can define and develop its role in the cyber domain and identify how specific segments of the service need to transform.

The end product of the mission-capability-package process would contain concepts of operations, command and force structures, corresponding doctrine, required training and education, technology, and systems with a support infrastructure designed and tailored to accomplish specific missions. The Air Force will best harness the emerging technologies of

the cyber domain by applying a mission-capability-package approach to coevolve the way it organizes, trains, equips, and fights with portions of its force. Figure 6 depicts the development process for the mission-capability package.

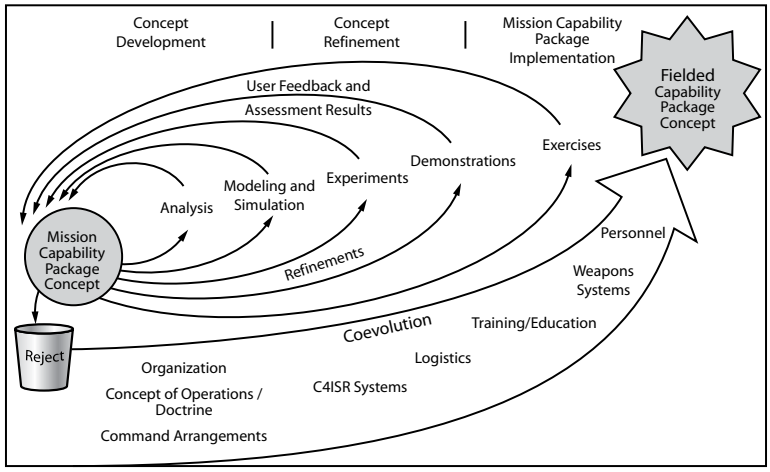


Figure 6. Process for the mission-capability package. (From David Alberts, *Information Age Transformation: Getting to a 21st Century Military* [Washington, DC: Library of Congress, March 2003], 76.)

The mission-capability-package process will assist the Air Force in understanding the implications of emerging cyber technologies and concurrently developing the necessary changes in other areas, thus ensuring a holistic approach. As the Air Force begins to employ the mission-capability package to take advantage of the cyber domain, it must consider essential factors that will contribute to its success in planning strategy as well as in building and organizing forces.

Critical Factors

> *Cyberspace is increasingly critical and inseparable from our national power and interests. . . . It is appropriate . . . to develop both a cyber power and a space power theory.*
>
> *—2006 Quadrennial Defense Review*

Although the Air Force changed its official mission statement to include flying and fighting not just in air and space but in cyberspace as well, the service is not yet postured to fulfill this mission.[112] Forming policy and changing mission statements are not enough—a great deal of work will have to take place to realize these capabilities.

Fortunately, the new mission statement goes beyond simply stating that the Air Force is going to operate or "fly" in cyberspace. Air Force leadership has expanded upon this basic description by directing the service to develop cyber strike packages and provide combatant commanders a full range of constantly available cyber effects.[113] These effects are designed to be integrated into combatant commanders' operational plans and into the strategic plans of the nation as a whole. In order to achieve the concrete effects and integration that a combatant commander would require for an operational plan, the Air Force will need to make significant changes to its existing cyber functions.

Much work lies ahead for the Air Force as it simultaneously lays claim to a role as lead service within the DOD for cyberspace activities. Because of the vastness and chaotic organization of the Internet, effectively employing cyber power on a global scale will require the Air Force to fundamentally change the way it views that power. It can no longer view cyber power solely as an adjunct to airpower and will have to fundamentally reorganize and strengthen the elements of cyber power that it currently has to execute that function. The secretary and chief of staff of the Air Force have moved things in this direction in a memo describing the new Air Force Cyber Command as both a supported and supporting component of a joint force—a first step in developing "cyber-mindedness."[114]

Constituting a Cyber Warfare Corps. The Air Force must retain appropriate skills in its workforce in order to support its cyber activities. Recruiting and retaining personnel with cyber skills such as computer programming and hardware development should be given top priority. In fact, appropriately trained personnel are the bulk of the expense involved in acquiring cyber capabilities in the case of network-warfare operations because the weapons involved are essentially software, and the test ranges are generally comprised of commonly available hardware and networks.

In contrast, the other two mission areas conducted within the EM environment—electronic warfare and directed energy—require both uniquely specialized hardware and skills. Development of all these skills should be inserted within the top 10 priorities on the Air Force's priority list of network-defense requirements.

While it is important that members of the initial cyber cadre be carefully selected from other disciplines, it is equally important that a small set of core cyber career fields be created to ensure that cyber theory can develop freely. Over time, cyber ideas must expand beyond theory to become a practical military art. Cyber practitioners must develop a new way of thinking—cyber-mindedness—similar to the air-mindedness that developed in the Army Air Corps so many years ago. Cyber-mindedness must become institutionalized in order to ensure that new theories of cyber power are developed.

In order to be truly effective in institutionalizing cyber power, the Air Force will have to adapt its culture to accept such unconventional warriors. The current cultural skepticism of the value and efficacy of cyber options in the military must be turned around. Though rarely articulated, many in the military view the impact and relevance of cyber attacks on the US military to date as at best minor. However, the risks of continuing to hold this view are growing. The military has become increasingly dependent on unclassified network connectivity for ordering parts for warplanes, ships, and tanks. Coupled with the rapid and effective development of offensive cyber capabilities by peer competitors such as China, failing to recognize the threat could have grave consequences for the exercise of US power.[115] Furthermore, this dismissive attitude holds back the development of the very corps of cyber professionals that can improve cyber weapons. The desired end state is to create a professionally trained and credentialed cyber career force with a fully developed theory of cyber power and the associations with the commercial computer industry it needs to be effective.

Training for Cyber Combat. As mentioned in the previous paragraph, it is not enough simply to set up a cyber corps. Cyber-related education is required prior to entry into federal service, and mission-specific training is required before a new cyber recruit is permitted to participate

in operations. Investments in this area should be heavy, as are the service obligations for those whose education and training are funded by the Air Force.

Large numbers of scientists and engineers with degrees in fields such as electrical engineering, computer science, and physics will have to be recruited directly from college. These personnel can be attracted to federal service through scholarships and encouraged to study specific subparts of these general sciences by offering research grants to promote focus on cyber-related capabilities in critical demand. Special retention bonuses and incentives will have to be offered to prevent military cyber professionals from leaving the service for more lucrative commercial jobs in cyber security. Also necessary is the creation of a separate pay scale for Air Force civilian cyber professionals, similar to the current scientist and engineer scales, to ensure retention of their critical skills. Access to certain capabilities may be possible only through the university system or academic community. In those cases, our existing research scientists and engineers should be permitted to work with those communities to obtain the necessary expertise until it can be created organically within the Air Force.

After acquiring the educated talent, the Air Force has to administer adequate and focused cyber training. That will require creation of a raft of specialty cyber-training classes and the instructional corps to administer them. Much of the training could be conducted virtually, of course, but the nature of cyber operations may require other types of nontechnical training. These additional training requirements are traditionally associated with clandestine or special operations forces and are necessary to enable sensing or offensive operations. The major subcategories of required training align with the three principal missions conducted in the EM environment: network warfare, EW, and directed-energy operations. Each of these specialties, however, will need training that facilitates a thorough understanding of their interdisciplinary relationships and ensures the free flow of critical information among them.

The acquisition of talent and training should be carefully articulated by Air Force Cyber Command. However, recruiting, educating, and training alone are not enough to ensure success. A corps of cyber professionals who are appropriately organized, equipped, and funded is also required.

Organizing Cyber Forces. Just as the establishment of a separate Air Corps was necessary for the full development of airpower theory and air-mindedness, so is the establishment of a cyber command an important step in developing cyber power. The US Army Air Corps provided the sort of immersion in air thinking needed for theories of airpower to develop unconstrained by its ties to ground power. Air Force Cyber Command will create the same sort of environment for the development of cyber power. The most recent direction from the Air Staff, the cyber "Go Do" letter, designates the Eighth Air Force commander as the commander of Air Force Cyber Command.[116]

Below the command level, however, in order to be effective, Cyber Command will need to be organized in ways to which the Air Force is not accustomed. Cyber warriors operate in an environment unique to the Air Force experience. For example, though defensive measures are critical in cyberspace, the irrelevance of distance and the speed of cyber operations already make it clear that the advantage in cyberspace goes almost entirely to the offense.[117] Even cyber defense has an offensive orientation. These and other characteristics of cyberspace will drive the need for cyber warriors to organize rapidly into dynamically formed teams of highly skilled experts from around the world, equipped with the latest tools and concepts of employment to deal with threats that will emerge from them. Cyber warriors will have to be permitted to train, organize, and equip in ways more appropriate to operating in cyberspace than current hierarchical military structures permit. These demand dynamic organizations, training, and assignment approaches that, although nontraditional, will serve to institutionalize cyber-mindedness within the Air Force and improve its effectiveness.

Cyber Command will provide a way for the Air Force to streamline presentation of cyber forces to US Strategic Command and provide a central focal point for coordination of cyber-related budgets and professional development. Because of the distributed nature of cyber power, the consolidation of existing centers of excellence is not only unnecessary but also undesirable. It is actually preferable that Cyber Command have several geographically separated operating locations, both to protect its capabilities and to enhance the diversity of options developed.

Cyber-Weapon Funding. Dedicated funding for professional research and design of cyber weapons and payloads is critical to delivering the options needed by the combatant commanders. According to a famous quotation by Brig Gen William "Billy" Mitchell, the first essential of airpower is preeminence in research. As technologically based as airpower is, this statement is even truer of capabilities in the virtual world of cyberspace. Because the advantage in cyberspace goes to the offensive, early development of new offensive cyber capabilities cannot be ignored. The speed and surprise of new cyber capabilities are novel; equally novel research and design approaches must be undertaken. In order to meet this challenge, the Air Force must change its approach to and funding of research and design.

The service must fund, build, and maintain a distributed capability to rapidly generate and integrate new cyber-attack weapons, and just as rapidly counter an adversary's new cyber weapons. First and foremost, this will require the identification of existing personnel and the acquisition and development of additional personnel with the right cyber skills. These personnel must be equipped with a robust "cyber range" to effectively perform rigorous research, development, and testing of new cyber capabilities and countermeasures. The best way to attain this capability early and at least expense is to connect all individual network test ranges currently operated by the Air Intelligence Agency; Rome Laboratories; Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center; and other Air Force units worldwide. Rough investment estimates to jump-start cyber capabilities for the first five years of Air Force Cyber Command total approximately $620 million, with fully one-third of that amount going to cyber recruitment and training.

Air Force Materiel Command is already engaged in a major research effort at its Rome Research Site to acquire cyber craft, a cyber analog to aircraft (table 15), but the effort is in dire need of additional funding.[118] The goal of this research is to create small, mobile, and highly autonomous programs capable of carrying out ISR as well as defensive and offensive cyber activities; it represents a best practice for developing future capabilities that would deliver cyber-weapon payloads to our adversaries. These agents will have to be simple, scalable, reliable, and provable.

Table 15. Kinetic air and space versus cyber craft

Kinetic Warfare (Characteristics)	*Cyber Warfare (Characteristics)*
Air and space vehicles: unmanned combat air vehicles	Cyberspace vehicles: cyber craft
Flight medium: air and space	Flight medium: cyberspace
Weapons: missiles and bombs	Weapons: viruses and worms
Desired effect: destroy target	Desired effect: destroy, degrade, and co-opt
Control: air/space/ground movement	Control: network links that support enemy air/space/ground movement
Low probability of intercept: stealth (physical)	Low probability of intercept: stealth (software)
Low probability of detection: terrain masking	Low probability of detection: network masking
Home base: predetermined airfield	Home base: any cyberspace portal
Logistics: heavy, continual	Logistics: light, infrequent (software)

Source: Dr. Kamal Jabbour, "RRS IF Directorate Mission Brief" (lecture, Air Force Research Laboratory Rome Research Site, Rome, NY, 14 September 2006).

Additional investment is required to surmount many technical challenges to the development of future capabilities, including radio-frequency and network penetration, intrusion detection, program development, size, and complexity, as well as artificial intelligence and morphing. In order to allow adequate funding for these efforts and prevent competition for resources from delaying cyber-development efforts, Air Force Cyber Command should be empowered by the Congress to budget separately to organize, train, and equip in a way similar to US Special Forces Command. This will ensure that existing Air Force programs are not adversely affected by the increased funding demands of developing cyber capabilities.

Air Force efforts in research and design should be coordinated with those of other government agencies. The 2003 *National Strategy to Secure Cyberspace* called for creation of a consolidated cyber research and development priority list that would ensure unity of effort and prevent duplication within the US government.[119] Sharing and deconflicting research efforts would conserve every agency's funds and answer critics such as the Government Accountability Office.[120]

It is only through full and rigorous development that combatant commanders' confidence in cyber weapons will increase sufficiently to employ them routinely and demonstrate their effectiveness. However, use of cyber options faces both legal and cultural challenges. The legal status of using cyber capabilities as weapons under the Geneva conventions remains unclear.[121] If the status is not resolved, combatant commanders will continue to avoid the application of cyber options.[122] This is clearly a subject that requires further consideration. In the absence of definitive international guidelines, clear and specific directives that delegate the authority to use cyber options to combatant commanders and other US government agencies are critical to enabling the application of cyber power.

Concluding Thoughts

> *It is a dangerous conceit to believe that a valid military concept can be developed and presented to the institution without undergoing this [military concept] development process. That said, sometimes it may be possible to commit to a concept and then develop it along the way. This approach invariably will suffer from trial and error, but may be necessary depending on circumstances.*
>
> —John Schmitt
> *A Practical Guide for Developing and Writing Military Concepts*

Schmitt's comment describes how the Air Force rolled out its vision of cyberspace operations. The service announced in late 2005 that its mission statement had changed and now included the term *cyberspace*. That announcement sent the institution reeling into debates concerning what the word meant. Nevertheless, the presentation of the concept without fully developing its implications was an astute way of avoiding the perpetual staffing and debate that all too often eradicate a new idea before it can realize any measure of its potential.

This research paper is intended to serve as an instrument that assists in developing a conceptual foundation for cyberspace operations, looking through the lens of the Air Force Concept Development framework. In applying that framework,

it has examined the attributes of cyberspace operations, proposed a focused definition of the term, described the current cyber situation and trends, illustrated cyber capabilities and effects, assessed the conduct and character of war in cyberspace, and, finally, examined recommendations for the way ahead, including a methodology and critical factors.

In an effort to contribute to the dialogue concerning the development of the cyber domain as part of the Air Force mission, this paper has highlighted the following issues for consideration:

1. War fighters need to be able to fully embrace cyberspace as a war-fighting domain. They need to be able to have confidence in planning and executing cyber tasks, applying cyber capabilities, and integrating operations in cyberspace with other domains in order to achieve intended effects.

2. The Air Force must clearly understand and characterize the digital-data environment; data constructs, tools, applications, and transport; and the ways one can know and use data in the context of offensive and defensive military operations.

3. Before the Air Force can effectively lead in the cyber domain, it must first fully understand the current US cyber situation. The service must examine current cyber conditions, analyze cyber threats, dissect current vulnerabilities, and clearly define how and where it can contribute to the national cyberspace strategy.

4. The principles of war are supported through the application of cyber capabilities, both directly and as enablers. Cyberspace capabilities do not change the nature of war.

5. Effective cyberspace operations are possible only with appropriately trained personnel, hardware and software tools that offer a mix of capabilities, cyberspace battle-management rules of engagement, measures of effectiveness, and sufficient time to employ specialized ISR functions.

6. Cyberspace capabilities must be fully coordinated with capabilities offered in other war-fighting domains.

7. A thorough concept of operations is absolutely fundamental to successfully planning strategy, building and organizing forces, and resourcing actions required in the cyber domain of warfare.

8. How well the Air Force harnesses the power of cyberspace in support of US national interests will be determined by the methodology it employs to define its role in the cyber domain.

9. Recruiting and retaining personnel with cyber skills such as computer programming and hardware development should be given top priority.

10. Large numbers of scientists and engineers with degrees in fields such as electrical engineering, computer science, and physics will need to be recruited directly from college to provide the skills needed for cyber missions.

11. The current cultural skepticism regarding the value and efficacy of cyber options in the military must be turned around.

12. Dedicated funding for professional research and design of cyber weapons and payloads is critical to delivering the options needed by combatant commanders.

This type of dialogue and input from various sources is critical to the development and eventual acceptance of cyberspace as a war-fighting domain. According to the Defense Adaptive Red Team's report, *A Practical Guide for Developing and Writing Military Concepts*,

> very few military concepts are created initially in full form or fully realized in their first incarnations. Like most ideas, military concepts tend to form iteratively and incrementally over time. This is no criticism of concept developers, but simply a reflection of the limits of human foresight. Developing a concept is not like building a house, in which the final result is fully blueprinted at the beginning of the process. Instead, concept development is more often a process of exploration and experimentation and tends to unfold as a hypothesis-antithesis-synthesis dialogue.[123]

Notes

1. Secretary and chief of staff of the Air Force to the Airmen of the United States Air Force, letter, 7 December 2005.

2. US General Accounting Office, *Information Security—Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, DC: Government Printing Office, 1996), 33; and US Department of Defense, *Joint Net-Centric Campaign Plan* (Washington, DC: Joint Chiefs of Staff, October 2006), http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf.

3. David S. Alberts, *The Unintended Consequences of Information Age Technologies: Avoiding Pitfalls, Seizing the Initiative* (Washington, DC: National Defense University, 1996), 22.

4. Secretary of Defense, *Information Operations Roadmap* (Washington, DC: Department of Defense, 30 September 2003), 6, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf. Document is now declassified.

5. Michael W. Wynne, secretary of the Air Force (address, C4ISR Integration Conference, Crystal City, VA, 2 November 2006), http://www.af.mil/library/speeches/speech.asp?id=283.

6. National Security Agency, "What Is Signals Intelligence?" http://www.nsa.gov/sigint (accessed 8 October 2006).

7. Department of Defense, *Joint Net-Centric Campaign Plan*.

8. David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004), 91–94.

9. CDR Lou Anne DeMattei, USNR, *Information Operations Doctrine: Service Perspectives*, research paper (Norfolk, VA: Joint Forces Staff College Advanced Joint Professional Military Education, 11 April 2004).

10. Briefing, Dr. Lani Kass, subject: Cyberspace: A War Fighting Domain, Air Force Association Air and Space Conference 2006, Washington, DC, 26 September 2006, http://www.afa.org/media/scripts/ppt_pdf/AFACyberspaceTaskForceBrief.pdf; and Wynne, address, C4ISR Integration Conference.

11. Joint Publication (JP) 3-0, *Joint Operations*, 17 September 2006, xi.

12. Secretary and chief of staff of the Air Force to Headquarters ACC, AETC, AFMC, and AFSPC, memorandum, 6 September 2006.

13. Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 11 January 2005, 1–5.

14. Dr. Kamal Jabbour, "RRS IF Directorate Mission Brief" (lecture, Air Force Research Laboratory, Rome Research Site, Rome, NY, 14 September 2006).

15. George J. Stein, "Information Warfare," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Alan D. Campen et al. (Fairfax, VA: AFCEA International Press, May 1996), 177.

16. AFDD 2-5, *Information Operations*, 3–5.

17. Ibid., 5.

18. Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Viking Penguin, September 2005).

19. David A. Fulghum, "Electronic Stew," *Aviation Week and Space Technology*, 29 January 2007, 34.

20. Brig Gen William T. Lord, *U.S. Air Force Concept of Operations for Information Operations*, 6 February 2004, 11.

21. Josh Rogin, "Air Force to Reorganize Intell Community," *Federal Communications Week*, 12 January 2007, http://www.fcw.com/article97349-01-12-07 (accessed 27 January 2007).

22. John F. Schmitt, *A Practical Guide for Developing and Writing Military Concepts*, Defense Adaptive Red Team Working Paper no. 02-4 (McLean, VA: Hicks and Associates, December 2002), 12, http://www.dtic.mil/jointvision/dart_guide.pdf.

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

24. US Department of Defense, *National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, March 2005), 16.

25. Wynne, address, C4ISR Conference.

26. Kass, briefing.

27. Martin C. Libicki, *Defending Cyberspace and Other Metaphors* (Washington, DC: National Defense University, February 1997), 39–40.

28. Lonsdale, *Nature of War*, 182.

29. Robert D. Steele, *Information Operations: Putting the "I" Back into DIME* (Carlisle, PA: US Army War College, 2006), 36–37.

30. Dr. Joe Strange, "Understanding Centers of Gravity and Critical Vulnerabilities" (address, Air War College, Maxwell AFB, AL, 28 November 2006).

31. Michael S. Loescher et al., *Proteus: Insights from 2020*, comp. Pamela H. Krause (Washington, DC: Copernicus Institute Press and Michael S. Loescher, 2000), 6–46.

32. *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), ix, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

33. USA Patriot Act, 107th Cong., 1st sess., H.R. 3162, sec. 1016, 24 October 2001.

34. *National Strategy to Secure Cyberspace*, viii.

35. Ibid., 5.

36. United States Computer Emergency Readiness Team, http://www.us-cert.gov.

37. *IC3 2005 Internet Crime Report, January 1, 2005–December 31, 2005* (Washington, DC: Federal Bureau of Investigation, National White Collar Crime Center, n.d.), http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf.

38. Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York: McGraw-Hill / Osborne Media, 2003), xv.

39. Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service Report for Congress (Washington, DC: Library of Congress, 1 April 2005).

40. *Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security*, 108th Cong., 2nd sess., 24 February 2004, http://www.fbi.gov/congress/congress04/lourdeau022404.htm.

41. Steven Hildreth, *Cyberwarfare*, Congressional Research Service Report for Congress (Washington, DC: Library of Congress, Government Printing Office, June 2001).

42. *Statement for the Record before the Joint Economic Committee on Cyber Threats and the U.S. Economy by John A. Serabian, Jr., Information*

Operations Issue Manager, Central Intelligence Agency, 106th Cong., 2nd sess., 23 February 2000.

43. Office of the Manager, National Communications System, "The Electronic Intrusion Threat to National Security and Emergency Preparedness Internet Communications: An Awareness Document" (Arlington, VA: National Communications System, December 2000), http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf.

44. *National Strategy to Secure Cyberspace*, 5.

45. United States Computer Emergency Readiness Team.

46. Ibid.

47. Ibid.

48. Department of Homeland Security, National Institute of Standards and Technology, "National Vulnerabilities Database," http://nvd.nist.gov.

49. Ibid.

50. *National Strategy to Secure Cyberspace*, x–xii.

51. *Homeland Security Act of 2002 and E-Government Act of 2002: Federal Information Security Management Act (FISMA)*, 108th Cong., 1st sess., H.R. 2458, 7 January 2003.

52. *FY 2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* (Washington, DC: Office of Management and Budget, 1 March 2006).

53. Lincoln's Second Annual Message to Congress, 1 December 1862, http://teachingamericanhistory.org/library/index.asp?document=1065.

54. Stuart J. D. Schwartzstein, ed., *The Information Revolution and National Security: Dimensions and Directions* (Washington, DC: Center for Strategic and International Studies, 1996), 37–180.

55. Air Force Policy Directive (AFPD) 10-28, *Air Force Concept Development*, 15 September 2003.

56. Ibid.

57. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 117–18.

58. Lonsdale, *Nature of War*, 216–17.

59. Sun Tzu, *Art of War*, trans. Lionel Guiles, 1910, http://etext.library.adelaide.edu.au/mirror/classics.mit.edu/Tzu/artwar.html (accessed 28 October 2006).

60. Schmitt, *Practical Guide*, 14–15.

61. JP 3-0, *Joint Operations*, IV-8.

62. Lonsdale, *Nature of War*, 180.

63. Douglas H. Dearth and Charles A. Williamson, "Information Age / Information War," in *Cyberwar: Security, Strategy and Conflict*, 26–28.

64. Jeffrey R. Cooper, "Another View of Information Warfare," in *Information Revolution and National Security*, 124; and Daniel Goure, "The Impact of the Information Revolution on Strategy and Doctrine," in *Information Revolution and National Security*, 220.

65. Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," in *Cyberwar: Security, Strategy and Conflict*, 34–42.

66. Michael Vlahos, "The War after Byte City," in *Information Revolution and National Security*, 100–106.

67. Alberts, *Unintended Consequences*, 21–22.

68. JP 3-0, *Joint Operations*, II-20.

69. Ibid., II-2.

70. Lord, *U.S. Air Force Concept of Operations*, 3.

71. William J. Bayles, "The Ethics of Computer Network Attack," *Parameters*, Spring 2001, 44–58.

72. Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (Washington, DC: Joint Chiefs of Staff, June 2000), 8–10, 22, 23.

73. JP 3-13, *Information Operations*, 13 February 2006, GL-6.

74. Kevin D. Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis: Wiley Publishing, 2002), 31.

75. Dr. Paul W. Phister et al., *CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment* (Rome, NY: Air Force Research Laboratory, Information Directorate, 23 February 2006), 5–6.

76. Stuart McClure, Joel Scrambray, and George Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, 5th ed. (Emeryville, CA: McGraw Hill / Osborne, 2005), 7.

77. International and Operational Law Department, Judge Advocate General's Legal Center and School, *Army Operational Law Handbook 2002*, chap. 20, "Information Operations," 3.

78. Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers* (Indianapolis: Wiley Publishing, 2005), 62.

79. McClure, Scrambray, and Kurtz, *Hacking Exposed*, 19.

80. Donald L. Pipkin, *Halting the Hacker: A Practical Guide to Computer Security*, 2nd ed. (Upper Saddle River, NJ: Prentice Hall, 2003), 174.

81. McClure, Scrambray, and Kurtz, *Hacking Exposed*, 78.

82. John Chirillo, *Hack Attacks Revealed: A Complete Reference with Custom Security Hacking Toolkit* (New York: John Wiley and Sons, 2001), 45.

83. McClure, Scrambray, and Kurtz, *Hacking Exposed*, 186.

84. Ibid., 175.

85. Ibid., 189.

86. Ibid., 190.

87. International Relations Research Center, "Wired Warfare: Computer Network Attack and Jus in Bello," *IRRC Review* 84, no. 846 (June 2002): 396–98.

88. Lord, *U.S. Air Force Concept of Operations*, 14.

89. Leigh Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's, 2004), 84.

90. David Farmer and W. Z. Venema, "Improving the Security of Your Site by Breaking into It," *Porcupine.org*, 1 February 2003, ftp://ftp.porcupine.org/pub/security/index.html#documents.

91. Mitnick and Simon, *Art of Intrusion*, 41.

92. Information Assurance Technical Forum, *Defense in Depth* (Washington, DC: Government Printing Office, 2002), 7.

93. Honeynet Project, *Know Your Enemy: Learning about Security Threats*, 2nd ed. (New York: Addison-Wesley Professional, 2004), 40.

94. Kelvin Wong, "Implementing Security: Introduction to Hacking Methods and Ways of Counter-Measure," *Swinburne Review*, Winter 2005, 9.

95. Honeynet Project, *Know Your Enemy*, 50.

96. Joseph Giordano, "Cyber Operations: A Historical Perspective" (lecture, Air Force Research Laboratory, Rome Research Site, Rome, NY, 14 September 2006).

97. Ibid., 4.

98. Ibid.

99. Phister et al., *CyberCraft*, 8.

100. Hugo Cornwall, *Hacker's Handbook* (Philadelphia: E. A. Brown Co., 1986), 10.

101. International Relations Research Center, "Wired Warfare," 396–98.

102. Mitnick and Simon, *Art of Intrusion*, 76.

103. Gr@ve_Rose, "SYN-ful Experiment," *2600: The Hacker Quarterly* 22, no. 2 (Summer 2005), http://www.2600.com/code/222.

104. *DOD Information Operation Roadmap (IO Roadmap)*, 30 October 2003, 2.

105. Lt Col Richard A. Lipsey, "Network Warfare Operations: Unleashing the Potential," in *Netted Bugs and Bombs: Implications for 2010*, ed. Dr. Marsha J. Kwolek (Maxwell AFB, AL: Center for Strategy and Technology, December 2005), 19.

106. "Revolution in Military Affairs," *SourceWatch*, http://www.sourcewatch.org/index.php?title=Revolution_in_military_affairs.

107. Tim Benbow, *The Magic Bullet? Understanding the Revolution in Military Affairs* (London: Chrysalis Books Group, Brassey's Publishing, 2004), 19.

108. Ibid., 14.

109. Colin S. Gray, *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context* (Carlisle, PA: Strategic Studies Institute, February 2003), 49.

110. SMSgt Anne Proctor, "AF Launches Cyberspace Task Force," Air Force Print News, 6 April 2006, http://www.au.af.mil/au/awc/awcgate/af/cyberspace_task_force.htm (accessed 8 June 2007).

111. Department of Defense, Command and Control Research Program, http://www.dodccrp.org.

112. Reuters, "Air Force Makes Bid for Mission in Cyberspace," *Google News*, 3 December 2005, http://www.google.com.

113. Kass, briefing.

114. Secretary and chief of staff of the Air Force to Headquarters ACC, AETC, AFMC, and AFSPC, memorandum, 6 September 2006.

115. Bill Gertz, "Chinese Hackers Prompt Navy College Site Closure," *Washingtontimes.com*, 30 November 2006, http://washingtontimes.com/national/20061130-103049-5042r.htm.

116. Gen T. Michael Moseley, chief of staff, US Air Force, to Lt Gen Robert J. Elder, commander, Eighth Air Force and Air Force Cyber Command, memorandum, 2 November 2006.

117. Kass, "Cyberspace, War Fighting Domain."

118. Phister et al., *CyberCraft*, 5–6.

119. *National Strategy to Secure Cyberspace*, 20.

120. John Monroe, "Feds Still Lack Security Research Agenda," *FCW.com*, 1 November 2006, http://www.fcw.com/article96662-11-01-06-Web &newsletter=yes.

121. International Relations Research Center, "Wired Warfare," 367.

122. *DOD Information Operation Roadmap (IO Roadmap)*, 2.
123. Schmitt, *Practical Guide*, 22.