AIR WAR COLLEGE

AIR UNIVERSITY

FLYING AND FIGHTING IN CYBERSPACE

by

Mike Convertino, Lt Col, USAF
Lou Anne DeMattei, DIA
Tammy Knierim, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

23 February 2007

[Cleared for public release 4/27/2007, AU 07-228]

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government and is not to be reproduced or published without the permission of the Air War College Studies Directorate.

Contents

Page

DISCLAIMER CERTIFICATE ii

ILLUSTRATIONS VI

TABLES VII

INTRODUCTION 1

THE CYBER DILEMMA 3
- Bounding the Cyberspace Domain 5
  - Requirement for a New Framework 5
  - Physical Attributes 8
  - Domain Differentiation: Cyber versus Information Operations in Cyberspace 10
  - Broad Implications for Joint Military Operating Concepts 13
  - Effects in Cyberspace 14
- Implications for Command and Control, Network Operations, and ISR 15
- A New Military Problem and New Solutions 16
  - Missions that Assure Operations in Cyberspace 17
  - Time Horizon, Assumptions, and Risks 18
- Relevance and Concluding Thoughts 19

THE U.S. CYBER SITUATION – THE PERFECT STORM? 23
- Current Conditions in the Cyber Domain 24
  - Information Infrastructure and Critical Infrastructure 24
- Existing "Weather Fronts" – Cyber Threat Agents 27
  - Threat and Threat Agent Defined 27
  - Threat Agent Profiles 27
- Strong Tropical Disturbance Feeding Energy to the Weather Fronts *a.k.a. Cyber Vulnerabilities* 32
- Battling the Simultaneously Challenging Winds of Change
  - U.S. National Strategic Way Ahead 35
  - National Strategy 36
  - Government Report Card 37
  - The Air Force and the Cyber Domain 39

THE CYBERSPACE DOMAIN OF WAR 41
- Conduct of War in Cyberspace 42

The Classics 42
The American Way of War 43
Military Operational Design 44
The Role of Technology 45
Principles and Functions of War 46

OPERATING IN CYBERSPACE 50
Intrinsic Characteristics as a Unique Combat Domain 51
Broader Span of Effects 51
Surgical Precision 52
Stealthy/Low Probability of Detection 52
Non-attribution/Untraceable 52
Cyber Capabilities 53
Cyber ISR 53
Target System Identification and Profiling 55
Access and Installation of a Persistent Presence 56
Mapping of Enemy Systems and Data 57
Analyzing Adversary Capabilities 59
Determining Adversary Intentions 59
Attack/Retaliatory Strike Planning 60
Cyber Defense 60
Protection from Attack 62
Attack Detection and Attribution 63
Automated Attack Responses and Operator Alerts 64
Self-healing of Systems and Networks 64
Rapid Recovery after Attack 64
Cyber Attack 65
Cyber Attack Authorization 67
Disruption of Adversary C2 Systems, Processes, and Data 67
Denying Access to Adversary Systems and Data 67
Degrading Adversary System Performance 68
Destruction of Adversary Data, Computers, Networks 68
Cyberspace Effects 68
Cyber ISR 70
Cyber Defense 71
Cyber Attack 71

RECOMMENDATIONS ON THE WAY AHEAD 74
Methodology 75
Cyberspace and the Revolution in Military Affairs Debate 75
Revolution in Military Affairs Defined 76
So What? 79
Cyberspace Operations as a Mission Capability Package 80
Critical Factors 82
Constituting a Cyber Warfare Corps 83
Training for Cyber Combat 85
Organizing Cyber Forces 86

Cyber Weapon Funding.....87

CONCLUDING THOUGHTS.....92

BIBLIOGRAPHY.....95

Illustrations

Page

Figure 1. Mapping of Ways and Means to Information Operations "Ends" (JP 3-13 IO Elements) 7

Figure 2. Mapping of Ways and Means to Information Operations "Ends" (Information Assurance Elements).....8

Figure 3. Cyberspace in a Conceptual Framework for War Fighting Domains 12

Figure 4. Levels of Impact for IW 14

Figure 5. Reported Security Incidents 1988-2003 28

Figure 6. Attack Sophistication v. Intruder Technical Knowledge 35

Figure 7. Principal Elements of Cyber ISR 55

Figure 8. Cyber Attack Trends.....61

Figure 9. Mission Capability Package Process 82

Figure 10. Kinetic Air and Space vs. Cyber Craft Comparison.....89

Tables

Page

Table 1. Key Cyber Domain Assumptions 25

Table 2. U.S. Critical Infrastructure Sectors with Lead Agency 26

Table 3. Synopsis of Threat Agents, Methodologies, and Intent.....29

Table 4. Summary of Nation State Cyber Capabilities.....32

Table 5. Federal Computer Security Report Card 38

Table 6. Reports Findings and Recommendations 39

Table 7. Principles of War and Cyber Capabilities.....48

Table 8. Classes of Attack 63

Table 9. Common Cyber Attack Categories and Methods 66

Abstract

This research paper develops the foundation for a new military operating concept to "fight the net" in support of 8th Air Force requirements and 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 and 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 fully characterize cyber conditions, threats, and vulnerabilities, and clearly define how and where it can contribute to the national cyberspace strategy. Once the Air Force accomplishes 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 organizational, research and development, and human capital investments that the Air Force needs “to fly and fight” effectively in cyberspace.

Chapter 1

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.*[1]
>
> *- 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*."[2] 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,[3] published a standard definition for cyberspace in 2006.[4]

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.[5] 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 and doctrinal clarity and consensus on the ends, ways, and means of operating in cyberspace, and

has resulted in an unfocused foundation on which to plan strategy, build and organize forces, and resource endeavors. Consequently, the ability to develop, deliver, and employ sovereign cyber options that achieve and maintain advantage in the cyber domain, and thus assure information superiority, is encumbered. As a means to further evolve a conceptual foundation for "fighting the net,"[6] this research paper will apply the Air Force Concept Development framework to examine the unique attributes of cyberspace operations and propose a more focused definition of cyberspace. In that context, it will describe 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."[7] Finally, it will assess the conduct and character of war in cyberspace, and offer recommendations for future cyberspace capabilities, policies and military operating concepts based on that analysis.

---

[1] Michael Brown, "The Revolution in Military Affairs: The Information Dimension," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Alan D. Campen et al. (Fairfax, VA: AFCEA International Press, May 1996), 44, 51.
[2] Secretary of the Air Force and chief of staff, USAF, to the Airmen of the United States Air Force, letter, 7 December 2005.
[3] US General Accounting Office, *Information Security - Computer Attacks at Department of Defense Pose Increasing Risks* (Washington, DC: Government Printing Office, 1996), 33.
[4] 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.
[5] David S. Alberts, *The Unintended Consequences of Information Age Technologies: Avoiding Pitfalls, Seizing the Initiative* (October 1996; repr., Washington DC: National Defense University, 1996), 22.
[6] 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.
[7] 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.

Chapter 2

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.*[1]

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.[2] 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."[3] This definition implied that cyberspace is broader than the EM spectrum alone, and involves the use of data and the hardware that channels electromagnetic 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, anti-radiation, 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.[4] That diversity is reflected in

differences in joint and service doctrines, as well as the Department of Defense Directive, on Information Operations.[5] 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 of 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.

As well, fundamental inconsistencies exist among the cyber objectives that describe what effects the Air Force seeks to achieve through cyberspace operations: full spectrum dominance, control of the information environment,[6] 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" from shaping through strike and stabilization.[7] 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 and globally dispersed. However, its task of clearly and simply articulating what airman 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.[8] 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, and announced 8th Air Force as the new Cyber Command.[9]

Bounding the Cyberspace Domain

A common understanding of the physical attributes of cyberspace and a clear delineation of the specific elements of military 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, several key questions need to be addressed:

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 can and should be considered in the cyberspace operational domain?

Requirement for a New Framework

Neither Air Force nor joint doctrine currently define or distinguish a "cyberspace" domain. The Air Force is fully ensconced in the challenge of pinning down standard, delimited, consistent descriptions of cyberspace and cyberspace operating concepts. As a starting point, Air Force doctrine adopts a unique organizing construct for Information Operations (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."[10] 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, and comprised of cognitive, physical, and information *dimensions*. Current IO doctrine and operating concepts blur the distinction between physical and non-physical aspects of "domain,"

fail to distinguish between “content” and “non-content” 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). Non-aligned effects require capabilities that are functionally diverse. They complicate cyber capabilities development as well as cyber-related organizational management.

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

Mapping of Ways and Means to Information Operations "Ends" (JP 3-13 IO Elements)			
Ends	**Ways**	**Means (Non-content)**	**Means (Content)**
Effects to be achieved in any warfighting domain	*Synchronized application of capabilites*	*Capabilities to affect signals and non-content data actions*	*Capabilities to affect content data, information, knowledge, intelligence/insight actions*
Destroy system	Apply non-kinetic (cyber) capabilities as a principle method of offensive or defensive operations	Physical destruction of system or data - e.g., format hard drive	Not directly applicable as a first order activity
Disrupt information		Computer network operations, signal processing and EM spectrum management	Not directly applicable as a first order activity
Degrade C2/C2 systems and information collection means		Computer network operations, signal processing and EM spectrum management	Not directly applicable as a first order activity
Deny access to critical information, systems, services		Computer network operations, signal processing and EM spectrum management	Not directly applicable as a first order effect
Deceive (MILDEC)		Not directly applicable as a first order activity	Perception management achieved through data and information manipulation
Exploit C2 by gaining access to systems		Computer network operations	Information management
Influence adversary behavior		Not directly applicable as a first order activity	Interdisciplinary
Protect against espionage or capture		Information management (COMSEC)	Interdisciplinary (CI, INFOSEC, physical security)
Detect system intrusion		Computer network operations	Not directly applicable as a first order activity
Restore information/information systems to original state		Computer network operations	Not directly applicable as a first order activity
Respond to adversary attack or intrusion		Computer network operations	Not directly applicable as a first order activity

Figure 1. Mapping of Ways and Means to Information Operations "Ends" (JP 3-13 IO Elements)

To better enable development and integrated application of cyber capabilities ("means"), cyber effects need to be described 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 "information operations ends" (Figure 2). Similar to the IA construct, the Air Force Research Lab uses the seven layer Open System Interconnect (OSI) model and Transmission Control Protocol/Internet Protocol (TCP/IP) as an architecture to guide its research and development of cyber capabilities.[11] Taken together, these

illustrations show that a more homogenous set of cyber means can be described to achieve effects (“ends”) that are functionally aligned.

Mapping of Ways and Means to Information Operations "Ends" (Information Assurance Elements)			
Ends	**Ways**	**Means**	**Means**
Effects to be achieved in all warfighting domains	*Synchronized application of capabilites*	*Capabilities to affect signals and non-content data actions*	*Capabilities to affect content data, information, knowledge, intelligence actions*
Authentication	Apply non-kinetic (cyber) capabilities as a principle method of offensive or defensive operations	Not applicable as a first-order activity	Computer network operations
Availability		Computer network operations, signal processing and spectrum management	Computer network operations
Confidentiality		Computer network operations	Computer network operations
Integrity		Computer network operations	Computer network operations
Non-repudiation		Computer network operations	Computer network operations

Figure 2. Mapping of Ways and Means to Information Operations "Ends" (Information Assurance Elements)

Physical Attributes

At a basic level, cyberspace shares some important characteristics with traditional domains of war. For a simple but illustrative analogy, cyberspace is a physical phenomena (the EM spectrum and data activities) that serves as a host and medium for implements of war (digital representation of data, information, knowledge, intelligence; electronic systems and networks; cybercraft), much the same as land hosts ground implements of war (soldiers, tanks, guns), the sea hosts maritime implements of war (sailors, ships, missiles), and air and space host airborne weapons of war (airmen, fighters/spacecraft, 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 non-kinetic effects are delivered using both non-content 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.

Data, the basic resource of cyber power, can be created at will and is essentially unlimited and unconstrained as a "material" component of warfare. Data itself can have veracity, while 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[12] -- a material component of the cognitive domain used to create influence effects. 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 command and control 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, and is not intended to be exclusive. For example, while the bulk of maritime operations take place in the physical environment of water, it is obvious that not all water-based maritime activities are naval warfare operations -- for example, port operations and law enforcement activities. Similarly, while the bulk of cyber operations take place in the physical environment of the EM spectrum, not all EM-based military activities should be characterized as cyberspace operations. Nor should all military activities that take place in what is currently referred to as the "information environment," conceptualized as a compilation of the physical, cognitive, and informational domains,[13] be characterized as information operations unless they directly involve the cognitive, content aspect of data and information.

Air Force Information Operations doctrine identifies three domains in which IO are conducted -- physical, information, and cognitive -- and three distinct types of IO -- influence operations, network warfare, and electronic warfare. Doctrine suggests that influence operations primarily occur in the cognitive domain of cyberspace, network warfare operations in the information domain, and electronic warfare (primarily) in the electromagnetic 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 non-content 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) and a limited subset of electronic warfare operations (occurring in the EM spectrum). "Influence" should be redefined broadly 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, electronic warfare should be addressed separately as a non-content, energy-based activity, rather than an IO activity, as it currently is.[14]

To address the definitional, consistency, and complexity dilemma, Figure 3 proposes a new conceptual framework for cyber operations within seven operational domains of war, one of which is cyberspace. This construct adopts a narrow definition of cyberspace operations focused on Computer Network Operations (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 COMINT (communications signals), ELINT (electronic/non-communications signals), FISINT (telemetry), and a small number of hybrids, and, for a range of functional and programmatic reasons, maintains a separate Information Assurance (IA) Directorate for CNO-Defense and related activities. The taxonomy has proven highly useful for manning, training, organizing, and equipping NSA's SIGINT and IA forces. Like the NSA model, Figure 3 distinguishes between informational- and energy-based activities occurring in the EM spectrum, associates the cyberspace domain with non-content 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).

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	Electromagnetic Spectrum	Cognitive
Missions/ Activities	Space Operations	Air Warfare	Land Warfare	Naval Warfare	Cyber (Digital Data) Operations (CNO)	Electronic Warfare (Signal processing, EM spectrum management, DE Ops)	Information and Perception Management Operations
Effects	Kinetic and non-kinetic 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/re-trievable information
Sample Organizational Elements	Space Command	Air Operations Center	Third Infantry Division	Sixth Fleet	Cyberspace Command	Army Electronic Warfare Division	Fourth PsyOps Group

Figure 3. Cyberspace in a Conceptual Framework for War Fighting Domains

As a concluding caveat on framework, it is important to consider the role and state of technology in the proposed construct. Figure 3 emphasizes a TCP/IP-centric differentiation for cyberspace because it is most consistent with state-of-the-art and state-of-practice applications. Energy-based electronic warfare 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,[15] the cognitive domain may very well be better conceived as a subset of cyberspace or the EM spectrum domains. 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 macro level, 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 non-military organizations that share cyberspace and support national security missions. As well, even in military operations, cyber operations are emphasized apart from EW as non-kinetic, non-combat "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 electronic warfare operations are executed are limited as a construct in helping to conceptualize and plan what war fighters do in cyberspace. Because current doctrine groups these functions as "information operations," our ability to integrate and apply their distinct capabilities in a logical, sequential, and integrated manner is often underemphasized, and sometimes ignored. For example, General Ronald Keys, Chief of Air Combat Command, made the following observation regarding potential application of F-22s as intelligence collectors supporting counterinsurgency 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.'[16]

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 Cooper's "Levels of Impact for IW" (Figure 4) is 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 RMA are further detailed in Chapter 6.

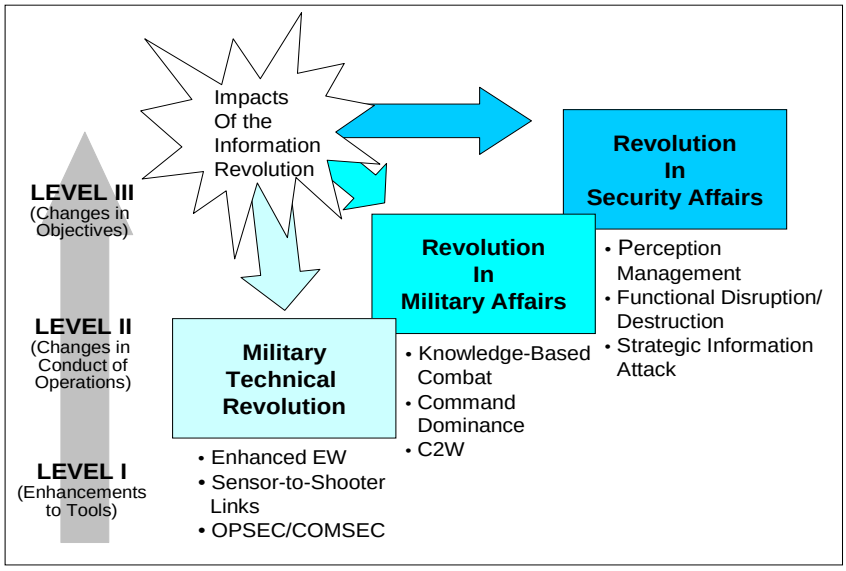

Figure 4. Levels of Impact for IW
(Reprinted from "Another View of Information Warfare," Jeffery R . Cooper, 1996)[17]

Effects in Cyberspace

The proposed conceptual framework identifies cyber operations as a computer network operations mission-level activity. As such, basic cyber capabilities should include cyber ISR,

cyber defense, and cyber attack using tools and approaches such as cybercraft 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 and protecting US interests should then include:

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

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

Implications for Command and Control, Network Operations, and ISR

Command and Control (C2) and Network Operations (NetOps) are both largely conducted in and dependent on cyberspace. C2 is a decision making activity and not a data activity, and as such, should not be considered to be a cyber capability, but rather a cognitive function. NetOps are essentially an information assurance activity provided through network defense, and are a basic task enabled through cyber defense capabilities. C2, NetOps, and ISR are currently characterized as "integrated control enablers" of Information Operations.[18] Current organizational constructs, as well as service, budgetary, and regulatory authorities, drive this characterization rather than applying classification based on their functionality and capabilities as military activities. The Air Force Chief of Staff announced plans in January 2007 to consolidate all intelligence, surveillance and reconnaissance programs under a new Air Force ISR command to begin to address alignment of integrated control enabling resources and

capabilities.[19] 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[20]

The ability to fly and fight effectively in cyberspace now and in the future hinges directly on proper definition, scope, conceptualization, and integration of tasks, effects, conditions, and objectives of operating in cyberspace. The military problem of fighting in cyberspace is new in that it is fundamentally a non-kinetic, non-violent approach to war. The fundamentally new, or at least underdeveloped, military problem in the cyber domain is scoping military application of cyber operations, and doing so primarily as a non-violent 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 applied as primary weapons of war, then basic concepts regarding use of force or threat of force to compel the enemy must change. While on the surface this approach appears straightforward, it should cause careful consideration on how the character and conduct of war are different in cyberspace.

Cyber capabilities for "fighting the net" and developed as weapons exist in a parallel, mostly integrated, "non-military" part of cyberspace, and are a second key consideration. This cyberspace slice is not necessarily distinguishable from a "joint cyber operations area" of war, and furthermore, many cyber weapons are indistinguishable from those capabilities applied as tools of non-military network management; societal informational activities, such as governmental, economic, political/ideological, religious; technology sharing; criminal activities; or even vigilante activities and individual thrill seeking on the net. For example, it is difficult to envision a routine civil application of a missile; it is entirely conceivable that commercial entities deploy cybercraft that collect against and target audiences to influence their behavior -- the same

cybercraft that would be applied in similar manner (and potentially against the same targets) by the military as weapons. Cyberspace is fundamentally a shared domain; cyber capabilities are inherently non-violent weapons and coexist 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.[21] 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 established a requirement for capabilities that enable operational freedom of action in cyberspace as a part of the "global commons," and linked the success of military operations with the ability to protect information infrastructure and data, and counter adversary exploitation of network vulnerabilities[22] -- in essence, to “assure” the ability to operate in cyberspace. Secretary of the Air Force (SECAF) Wynn further addressed this issue directly in remarks during a November 2006 conference 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 as follows:

1. Sustain military action to ensure freedom of access and usage of cyberspace;
2. Prevent illicit use of cyberspace; and
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.[23]

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. Assured cyber operations are further discussed in Chapter 2.

Time Horizon, Assumptions, and Risks

The target timeframe for operating concepts suggested by this study is 2009-2014, 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 U.S. center of gravity, and technology development and research resourcing.

While it may or may not be feasible to establish boundaries in cyberspace as a global domain, 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 2006 National Military Strategy for Cyberspace Operations, Dr. Lani Kass, Director of the Air Force Cyber Task Force, found that boundaries do not apply in cyberspace, and control of cyberspace is an essential task of the Air Force cyber mission.[24] Dr. Martin Libicki, renowned RMA and Information Warfare (IW) policy expert, asserted that cyberspace is ubiquitous and not owned nor defendable by the Department of Defense acting alone. As a result he finds that the concept of "forcible entry" does not exist in cyberspace in the same way as in other war fighting domains.[25] Dr. David Lonsdale, International Relations and IW expert, found that cyberspace and the information resident in it are increasingly becoming "territorialized" and therefore will eventually be controlled and defended.[26] In contrast, consider the very viable endeavors of Wikipedia, the Open Software Initiative, and Dr. Robert David Steele's concept of Open Source Intelligence,[27] which together,

demonstrate an open architecture for data, information, knowledge, and intelligence. 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 that global control is possible are at risk. This risk is further amplified by the dynamic nature of cyberspace, and the virtually unlimited capability to create new data and resources that are the target of cyber military operations.

Conventional wisdom holds that cyberspace and the information residing in it constitute a U.S. center of gravity (CG). Dr. Joe Strange, strategy and campaign planning expert, postulated that CGs must have the ability to "strike heavy or effective blows, and must offer resistance." [28] While a metaphor for cyberspace and information as a CG that meets these criteria is difficult to conceive, it is relatively easy to describe belief systems and their decision makers as such. Given this more nuanced understanding of CG characteristics, conventional wisdom regarding cyberspace and information as a CG may need reconsideration.

Technology assumptions are also 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 are closely related to technology assumptions, and should drive risk considerations.

Relevance and Concluding Thoughts

Clarity of words, definitions, and concepts is important and relevant. Simply put, 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. Until we can clearly conceptualize and describe this domain and operations in it, we will not be able to offer a viable, effective roadmap for the development and application of cyber capabilities. The full benefit of cyber power will not be embraced nor realized by war fighters, and worse, we will risk missing or losing completely the opportunity to seize and maintain the advantage of the cyber operating environment.

In the *Proteus* project sponsored by the National Reconnaissance Office (NRO), the "problem space" of the future was examined 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 information operations. It proposes that Internet be conceived as a parallel universe rather than simply a global network. To paraphrase,

> 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 is silent on intrinsic truth or falsehood. . . .
>
> In the progression from data through knowledge to insight, understanding what is knowable may be more important than differentiating between truth and falsehood.[29]

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 how data is knowable and usable in the context

of offensive and defensive military operations. Only then will an adequate conceptual foundation be available to properly evolve future operating concepts for flying and fighting in cyberspace.

---

[1] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004), 184.
[2] National Security Agency, "What is Signals Intelligence," http://www.nsa.gov/sigint/ (accessed 8 October 2006).
[3] 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.
[4] Lonsdale, *Nature of War*, 91-94.
[5] Lou Anne DeMattei, CDR, USNR, "Information Operations Doctrine: Service Perspectives" (research paper, Joint Forces Staff College Advanced Joint Professional Military Education, 11 April 2004).
[6] Dr. Lani Kass, "Cyberspace: A War fighting Domain" (briefing, Air Force Association Air & Space Conference 2006, Washington, DC, 26 September 2006), www.afa.org/media/scripts/ppt_pdf/AFACyberspaceTaskForceBrief.pdf.
[7] 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.
[8] Joint Publication 3-0 (JP 3-0), *Joint Operations*, 17 September 2006, xi.
[9] Secretary of the Air Force and chief of staff, US Air Force to HQ ACC, HQ AETC, HQ AFMC, HQ AFSPC, memorandum, 6 September 2006.
[10] Air Force Doctrine Document (AFDD) 2-5, Information Operations, 11 January 2005, 1-5.
[11] Dr. Kamal Jabbour, "RRS IF Directorate Mission Brief," (lecture, AFRL Rome Research Site (RRS), Rome, NY, 14 September 2006).
[12] 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.
[13] AFDD 2-5, 3-5.
[14] AFDD 2-5, 5.
[15] Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Viking Penguin, September 2005).
[16] David A. Fulghum, "Electronic Stew," *Aviation Week & Space Technology*, 29 January 2007, 34.
[17] Jeffrey R. Cooper, "Another View of Information Warfare," in *The Information Revolution and National Security Strategy*, ed. Stuart J. D. Schwartzstein (Washington, DC: The Center for Strategic and International Studies, 1996), 125.
[18] US Air Force Concept of Operations for Information Operations, 6 February 2004, 11.
[19] Josh Rogin, "Air Force to Reorganize Intell Community," *Federal Communications Week*, 12 January 2007, http://wwww.fcw.com/article97349-01-12-07, accessed 27 January 2007.
[20] John F. Schmidt, *A Practical Guide for Developing and Writing Military Concepts*, Defense Adaptive Red Team Working Paper #02-4 (McLean, VA: Hick & Associates, Inc., December 2002), 12.
[21] AFDD 2-5, 5.
[22] US Department of Defense, *National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, March 2005), 16.
[23] Gen Michael W. Wynne, secretary of the Air Force, US Air Force (address, C4ISR Conference, Crystal City, VA, 2 November 2006), http://www.af.mil/library/speeches/speech.asp?id=283.
[24] Kass, "Cyberspace: A War Fighting Domain," 26 September 2006.
[25] Martin C. Libicki, *Defending Cyberspace and Other Metaphors* (Washington, DC: National Defense University, February 1997), 39-40.
[26] Lonsdale, 182.
[27] Robert D. Steele, *Information Operations: Putting the "I" Back into DIME* (Carlisle, PA: U.S. Army War College, 2006), 36-37.
[28] Dr. Joe Strange, "Understanding Centers of Gravity and Critical Vulnerabilities," (address, Air War College, Maxwell AFB AL, 28 November 2006).

[29] Michael S. Loescher et al., *Proteus: Insights from 2020*, comp. Pamela H. Krause (Washington, DC: The Copernicus Institute Press & Michael S. Loescher, 2000), 6-46.

Chapter 3

The U.S. 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 1991 Halloween Nor'easter. This storm devastated the Atlantic seaboard for days, killed 12 people, and resulted in over a billion dollars in damage. The storm was not a hurricane so it did not elicit the normal hurricane warnings. Therefore, many on-shore citizens and deep-sea fishermen were caught 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" is the convergence of independent events that form an environment never experienced before. The current United States cyber situation involves diverse threat agents that if conflated with system vulnerabilities will create the cyber "perfect storm." Unless national strategies and policies are put into practice to change one or more of these contributing factors, the U.S. cyber perfect storm will have impacts that go far beyond property damage and shoreline erosion.

When the Air Force leadership revised their service's mission statement to say "fly and fight in air, space, and *cyberspace*," they 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 U.S. cyber situation pointing to the perfect storm. The Air Force must examine threat agents, dissect current vulnerabilities, prioritize credible threats, and clearly define how and where the Air Force can contribute to the national cyberspace strategy.

This chapter begins with the "current conditions" in the cyber domain by highlighting key definitions and assumptions. Next, it examines cyber threat agents as "existing weather fronts" and provides evidence identifying current U.S. cyberspace vulnerabilities -- the "strong tropical disturbance feeding energy to the fronts." After building the case for an impending "perfect storm," the final section of this chapter explores the U.S. strategic way ahead that is battling the "simultaneously challenging winds of change." Together these elements define the current U.S. cyber situation and point toward a perfect storm.

Current Conditions in the Cyber Domain

Weather forecasting is concerned with the analysis and interpretation of the evolution of atmospheric phenomena. As such, the science of weather forecasting relies on certain definitions and assumptions. Accurate forecasting in the cyber domain is similar to weather forecasting and therefore it is useful to provide a brief synopsis of the current environment in the cyber domain.

Information Infrastructure and Critical Infrastructure

> *"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 of IEEE-USA's Research and Development Policy Committee*

The U.S. information infrastructure is defined as interconnected computing and storage systems, mobile devices, software, wired and wireless networks, and related technologies.[1] Before examining threats to this infrastructure, certain cyber domain assumptions are outlined in Table 1 to provide a common reference point for discussion.

Table 1. Key Cyber Domain Assumptions

Key Cyber Domain Assumptions – The Current Conditions
☑ Information technology infrastructure is indispensable to public & private sector activities across the globe
☑ Interconnectivity exposes previously isolated critical infrastructures to the risk of cyber attacks mounted through the IT 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 U.S. 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 U.S. IT infrastructure and critical infrastructure is a matter of national and homeland security.

***Source*:** Data compiled from NSTC, GAO, CSIS, and PITAC reports and DHS Cybersecurity Strategy and the Strategy to Secure Cyberspace.

There is no doubt that increasing computer interconnectivity has revolutionized the way that much of the world communicates and conducts business. While 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. 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 U.S. *information infrastructure* and the U.S. *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."[2] A list of the 14 U.S. critical infrastructure sectors with their designated lead agency is provided in Table 2.

Table 2. U.S. 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 & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government	*Continuity of government* Department of Homeland Security *Continuity of operations* All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security*
Banking and Finance	Department of the Treasury
Chemical Industry	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interir

***Source*:** Office of Homeland Security. *National Strategy for Homeland Security*, Washington, D.C., GPO, July 2002.

Table 2 shows that the U.S. critical infrastructure sectors are substantial and composed of both private and public entities. The National Strategy to Secure Cyberspace stated that the common thread linking these diverse sectors together is the domain of cyberspace -- the "nervous" system that "controls the country."[3] It is this nervous system that requires national vigilance and safeguarding. These definitions and assumptions are 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 in the horizontal and vertical direction. In order to create a strong storm, these fronts must be strengthened by another force. Similar to a typical weather front, current cyber threat agents manifest themselves from every direction and are anxious to be fed energy in order to intensify and build into a much stronger storm. Much like successfully forecasting an incoming weather front, if the Air Force is to be 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 defined as "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."[4] As defined here, cyber threats not only involve an action but require actors (threat agents) to execute that action in order to exploit cyber weaknesses.

Threat Agent Profiles

The threat agents, those people or organizations who intend to exploit vulnerabilities, represent a huge growth industry. The frequency of cyber attack incidents is so commonplace that the U.S. federal government's center of Internet security expertise, the Computer Emergency Readiness Team (CERT), ceased reporting the number of incidents in 2004 because the overwhelming numbers provided little information to help assess the scope and impact of attacks.[5] 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 5 depicts the dramatic rise in *reported* incidents.

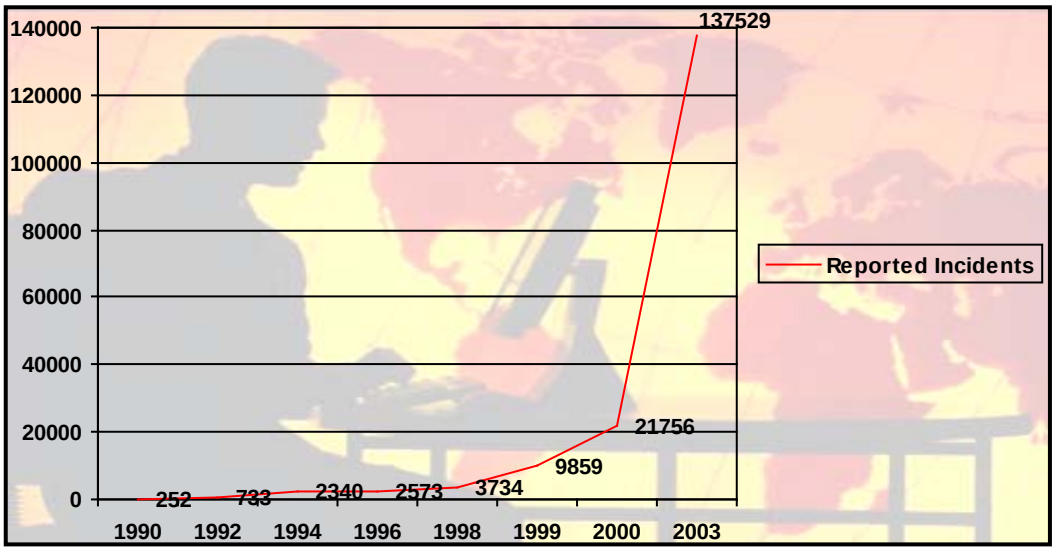

Figure 5. Reported Security Incidents 1988-2003
(Data compiled from the U.S. CERT, http://www.cert.org/)

There is no doubt from the data above that both the frequency and effectiveness of malicious cyber attacks are escalating. The threat agents executing these attacks are also evolving while multiplying and can be placed into four general profiles – hackers, organized crime, terrorists, and nation states. Table 3 provides a brief synopsis of threat agents, their methodologies and intent.

Table 3. 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, extortion.
Organized Crime	☒ Exploit online activity, hire hackers, bribe insiders. ☒ More structured/resources than hackers.	☒ Monetary gain.
Terrorists	☒ Hacking. ☒ Exploitation of Internet.	☒ Acquire information for planning physical or cyber attacks. ☒ Command and control.
Nation States	☒ Offensive cyber capabilities. ☒ Few have technical and operational capabilities for wide-spread impact.	☒ Espionage. ☒ Cyber warfare.

Source: Office of Homeland Security. *National Strategy for Homeland Security*, Washington, D.C., GPO, July 2002.

The most widely discussed category of threat agents is hackers. Hackers possess a collection of skills that allow them to break into systems for the simple challenge of the act or for more malicious intent. They may use their own code or easily accessible scripts to launch attacks or probes. There are many types of hackers -- botnet operators, phishers, and spammers to name a few. Botnet operators are hackers who 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 be individuals or groups that distribute unwanted e-mail with hidden information to sell products, conduct phishing scams, or implant spyware.

Recognizing the potential hackers have to perform tasks leading to monetary gain, organized crime is increasingly recruiting hacking services. The FBI's Internet Crimes Complaint Center (IC3) reported in 2005 that they processed over 228,000 cyber crime complaints, referred nearly 100,000 cases for criminal investigation, and estimated the total dollar loss from fraud at $183

million.[6] 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 federal government agencies or departments, 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 that 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."[7] Evidence of terrorist organizations' awareness and use of information technology and the cyber domain has grown since 2000. As physical and border security increase, terrorists may turn to cyber warriors or hacker services to engage in cyberterrorism against the U.S.[8]

Cyberterrorism is defined by the FBI 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."[9] Although there is some debate 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.

While terrorist groups currently lack the required resources, skill, and coordination to conduct large-scale cyberterrorism, traditional nation-states are actively building both offensive and defensive capacity to execute cyber warfare. According to a Congressional Research

Service report, the term "cyberwarfare" can be used 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.[10]

The previous chapter briefly discussed the concept of cyberspace and the information residing in it as possibly constituting a center of gravity. While this argument will be debated for some time, there is evidence today that the cyber domain is quickly becoming a focus for nation-states in posturing themselves for future warfare. John A. Serabian, Jr., Information Operations 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.[11]

There is little doubt that 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.[12]

In 2004, the Department of Homeland Security 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 cyber threat capabilities in order to dispel myths about the nature and degree of the cyber threat. Countries studied include China, India, Iran, North Korea, Pakistan, and Russia. Their findings are summarized in Table 4.

Table 4. Summary of Nation State Cyber Capabilities

	CHINA	INDIA	IRAN	N. 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 IT industry and/or technical universities	x	x	x		x	x
IT roadmap	Likely	x				
Information warfare units	x	x		x		
Record of hacking other nations						x

Source: Billo, Charles and Welton Chang. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*, Institute for Security Technology Studies, Dartmouth College, December 2004.

This section illustrated that cyber threat agents exist, take many forms, and are becoming stronger every day. There is no doubt that malicious cyber activity has increased dramatically and continues to proliferate. Having defined and assessed cyber threat agents as "incoming weather fronts," it is then important to examine vulnerabilities that feed these threats.

Strong Tropical Disturbance Feeding Energy to the Weather Fronts *a.k.a. Cyber Vulnerabilities*

In addition to tracking the moving weather fronts, a vigilant forecaster must watch for potential weather patterns with the potential to merge with and strengthen the storm. A strong tropical disturbance is defined as 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 they must watch these other weather patterns with the potential of colliding with and intensifying the front.

Current U.S. cyberspace vulnerabilities provide possible sources of additional energy to cyber threat agents thereby setting the stage for intensifying storm patterns. If the Air Force is to be effective in flying and fighting in cyberspace it must not only anticipate, assess, and prioritize cyber threat agents but it must also continually act to identify and block vulnerabilities that provide opportunity to those cyber threat agents.

A *vulnerability* is defined as a "flaw or weakness in the design or implementation of hardware, software, networks, or computer-based systems including security procedures and controls associated with the systems."[13] Without vulnerabilities there is no threat…but the U.S. information infrastructure is far from being vulnerability-free.

Technology gives users tremendous opportunities, access, and efficiency, and also provides attractive capabilities to various threat agents who intend to harm to users, society, the economy, and the country. Vulnerabilities are easy to exploit from anywhere across the globe. The U.S. information infrastructure is 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 the 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 computer systems vulnerabilities. The standard for information security vulnerability names was termed "common vulnerabilities and exposures" or CVE. According to Mitre, the definition of a universal vulnerability is a state in a computing system (or set of systems) which either allows an attacker to execute commands as another user, to access data that is contrary to the specified access

restrictions for that data, to pose as another entity, or to conduct a denial of service.[14] In addition to defining common terminology for vulnerabilities, Mitre defined the term "exposures." The definition of an exposure is a state in a computing system (or set of systems) which is not a universal vulnerability but 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.[15] Today, the CVE is sponsored by the National Cyber Security Division at the Department of Homeland Security whose objective remains to provide 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.[16]

In combination with the CVE national vulnerability naming standard, the National Institute of Standards and Technology maintains a national vulnerability database sponsored by the Department of Homeland Security Cyber Security Division/US-CERT. This comprehensive database combined all publicly available U.S. Government vulnerability resources and provided references to industry resources.[17] A quick search for statistics regarding vulnerabilities from 1988 to 2006 revealed a staggering increase from 2 to nearly 6,000.[18]

As vulnerabilities skyrocketed in the last several years, the attack sophistication, technical knowledge, and availability of malicious tools has also proliferated. Researched at the Software Engineering Institute at Carnegie Mellon University prepared a briefing in 2002 titled "Cyberterrorism" to characterize these trends. Their findings are summarized in Figure 6.

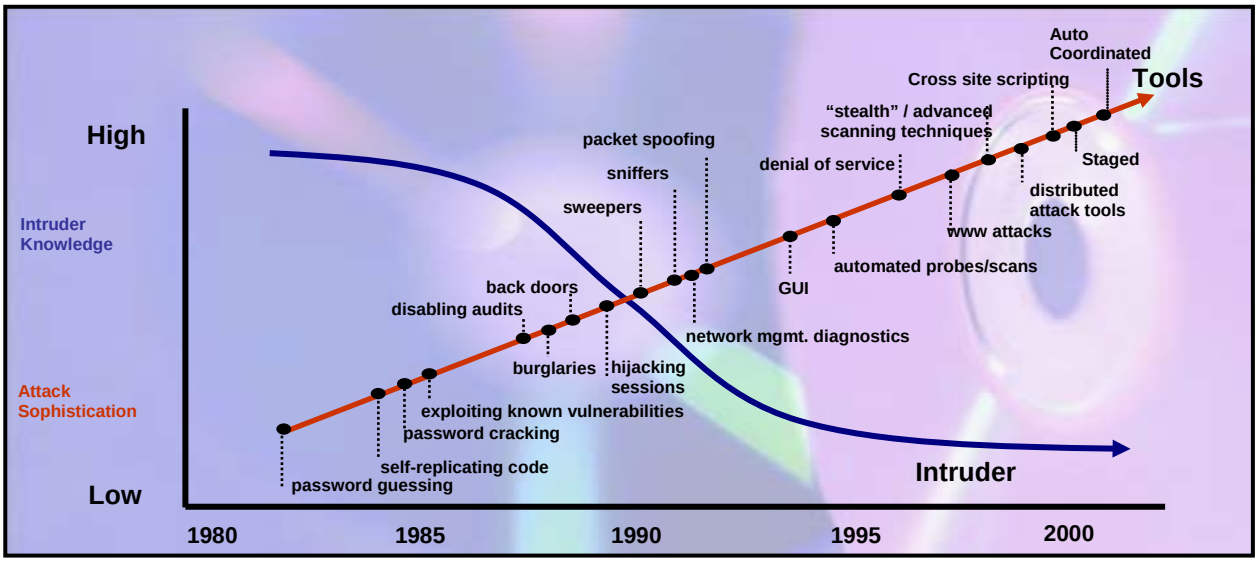

Figure 6. Attack Sophistication v. Intruder Technical Knowledge
(Source: Software Engineering Institute at Carnegie Mellon University)

The convergence of existing threat agents, vulnerabilities, attack sophistication and intruder technical knowledge is creating the conditions for a remarkable storm. The thunderclouds are forming. The Air Force must not only create a roadmap that anticipates, assesses, and prioritizes cyber threat agents. It must continually act to identify and mitigate vulnerabilities, and it must chart how it will fall in with the U.S. national strategic way ahead and existing Department of Defense cyberspace efforts.

Battling the Simultaneously Challenging Winds of Change
U.S. National Strategic Way Ahead

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 U.S. government tackles the challenge of mitigating risk in the cyber domain, conditions and circumstances are constantly and rapidly evolving. Even so, the U.S. government continues to pursue ways to secure cyberspace so that threat agents are unable to jeopardize national security.

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.*
>
> President George W. Bush
> *National Strategy to Secure Cyberspace*

The U.S. national policy concerning cyberspace security is clear as is the strategic way ahead. The challenge for governmental departments is how they implement and operationalize 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.* This strategy document outlined five national cyberspace security priorities:

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. Securing government's cyberspace
5. National security and international cyberspace security cooperation

The strategy also outlined explicit actions required by for 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
8. Develop Specific Criteria for Independent Security Reviews and Reviewers and Certification

The National Strategy goes on to highlight that the foundation for the government's cyber security required assigning clear and unambiguous authority and responsibility for security, holding officials accountable, and integrating those requirements into budget and capital planning processes.[19]

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 required government agencies to secure the information and information systems that support its operations and assets, including those provided or managed by another agency, contractor, or other source.[20] The act further required agency Chief Information Officers (CIO) and Inspectors General (IG) to report results of annual reviews to the Office of Management and Budget for their 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 OMB report to Congress dated 1 March 2006, the Department of Defense was scored among the lowest of the 24 government agencies or departments required to comply with FISMA. Based on the Chief Information Officer and Inspector General reports, the OMB found that DoD did not have an effective plan of action or milestones to address deficiencies in information security policies, procedures and practices.[21] The OMB also found that DoD process of certification and accreditation was "poor." Finally, the OMB highlighted that DoD was among the lowest percentage complete (0-50%) for system inventory. As a result, the Congressional Committee

on Government Reform gave DoD an overall "F" on its computer security report card for 2005, decreasing from the previous two years' "Ds".

Table 5. Federal Computer Security Report Card

FEDERAL COMPUTER SECURITY REPORT CARD	**16 FEB 2006**		
GOVERNMENT WIDE GRADE D+			
	2005	**2004**	**2003**
Department of Defense	**F**	**D**	**D**

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 Department of Homeland Security published *Cybersecurity for the Homeland*; the GAO published the *Critical Infrastructure Protection: DHS Faces Challenges in Fulfilling Cybersecurity Roles* and *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*. 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 6 summarizes some of the key findings and recommendations the reports have in common.

Table 6. Reports Findings and Recommendations

FINDINGS AND RECOMMENDATIONS	*Cybersecurity for the Homeland December 2004*	*Critical Infrastructure Protection DHS Faces Challenges in Fulfilling Cybersecurity Roles GAO Report May 2005*	*Federal Plan for Cyber Security and Information Assurance Research and Development April 2006*	*Critical Infrastructure Protection DHS Leadership Needed to Enhance Cybersecurity GAO Report 13 September 2006*
Coordinate w/private sector	X	X	X	X
Conduct Threat/risk assessments	X	X	X	X
Improve integration w/other agencies	X	X	X	X
Improve outreach/coordination	X	X	X	X
Increase R&D investments	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 highlighted documents.

As the federal government attempts to mitigate risk in the cyber domain, the key components for success are assessment, integration, investment, coordination, and partnerships -- no one agency can conquer this challenge alone.

The Air Force and the Cyber Domain

When the Air Force leadership revised their service's mission statement to say "fly and fight in air, space, and *cyberspace*," they acknowledged the importance of the cyber domain and recognized that to succeed in future conflicts they would need to focus on multiple domains. But before the Air Force can effectively lead in the cyber domain, it must first fully understand the current U.S. cyber situation. The Air Force must examine the current cyber conditions, analyze

the cyber threats, dissect the current vulnerabilities, and clearly define how and where the Air Force can contribute to the national cyberspace strategy. Once the Air Force accomplishes 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."[22]

---

[1] President, Strategy Document, "U.S. National Security to Secure Cyberspace." February 2003, ix.
[2] USA PATRIOT ACT, 107th CONGRESS, 1st Session H. R. 3162, Section 1016, October 24, 2001
[3] President, Strategy Document, "U.S. National Security to Secure Cyberspace." February 2003, viii.
[4] Ibid, 5.
[5] United States Computer Emergency Readiness Team, http://www.us-cert.gov/.
[6] Federal Bureau of Investigation, National White Collar Crime Center. *IC3 2005 Internet Crime Report, January 1, 2005 – December 31, 2005*. Washington D.C.
[7] Verton D, 2003, *Black Ice: The Invisible Threat of Cyber-Terrorism* (New York, NY: McGraw-Hill Osborne Media), xv.
[8] Clay Wilson, *Congressional Research Report: Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* 1 April 2005, Washington D.C., Library of Congress
[9] Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004, http://www.fbi.gov/congress/congress04/lourdeau022404.htm.
[10] Steven Hildreth, Congressional Research Service. *Cyberwarfare*, CRS Report for Congress. Library of Congress, GPO, June 2001.
[11] Serabian Testimony. 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, 23 February 2000, Washington D.C.
[12] Office of the Manager, National Communications System, "The Electronic Intrusion Threat to National Security and Emergency Preparedness Internet Communications: An Awareness Document." December 2000, Arlington, VA. http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf.
[13] President, Strategy Document, "U.S. National Security to Secure Cyberspace." February 2003, 5.
[14] United States Computer Emergency Readiness Team, US-CERT and CVE, http://www.us-cert.gov/.
[15] Ibid.
[16] Ibid.
[17] Department of Homeland Security, National Institute of Standards and Technology, "National Vulnerabilities Database," http://nvd.nist.gov/.
[18] Ibid.
[19] President, Strategy Document, "U.S. National Security to Secure Cyberspace." February 2003, x.
[20] *Homeland Security Act of 2002 and E-Government Act of 2002: Federal Information Security Management Act (FISMA)*, 108th Congress, First Session, HR 2458, 7 January 2003..
[21] Office of Management and Budget, *FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002,* Washington D.C., 1 March 2006. .
[22] Lincoln's Second Annual Message to Congress, December 1, 1862. http://teachingamericanhistory.org/library/index.asp?document=1065.

Chapter 4

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 [1]

Volumes of scholarly works have contemplated implications of the Information Age on national security, warfare, and military strategy for more than a decade. Nearly all concluded that the explosion in variety, volume, and velocity of information and associated technologies have birthed a profoundly new environment with dramatic implications for military operating concepts, and new methods of fighting that broaden the span of effects across the spectrum of war.[2] 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.

The emergence of the "information environment" and network centric warfare concepts 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 non-content cyber activities. New military operating concepts are therefore required.

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" in their formulation.[3] Accordingly, this chapter reviews the nature and conduct of war inclusive of the cyberspace domain and its impacts 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 "nature of war" is used to describe the fundamental qualities of war. The two bedrock theories describing the nature of war used to consider new military operating concepts are Carl von Clausewitz' *On War* and Sun Tsu's *Art of War*.[4] New cyber operating concepts are also considered in view of the "American Way of War," a characterization of war fighting that emphasizes American approaches to war.

The Classics

The 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.[5] Because war fighting in cyberspace is envisioned primarily as a non-kinetic, information-based approach, the concept of war in this domain as a Clauzewitzian conflict is indirect, but still highly relevant. 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.[6]

According to Sun Tsu, success or failure in war is determined by information. Sun Tsu held that complete knowledge of enemy and self are attainable, and therefore, enable selection of the correct strategy for success in battle, or perhaps will even yield victory without battle.[7] For Sun Tsu, violence is only a part of war, and engagement 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 Tsu's theories, and directly captures the concept of achieving information advantage and applying that to execute and win wars.

The American Way of War

The conduct of war in cyberspace plays to American strengths: the American approach seeks to control tempo and initiative through rapid global reach and agility; to neutralize adversary command and control capabilities; to apply deadly force with minimal collateral damage through precision strike; and to minimize exposure of forces through stand-off engagement and rapid establishment of air supremacy, all underpinned by advanced technology solutions.[8] Operating in cyberspace is a global activity that provides a broad span of effects ranging from benign presence through precision strike by employing non-kinetic solutions, and facilitating kinetic effects that are increasingly unconstrained by time and distance. The "shock and awe" strategy that delivered overwhelming military effects in Iraq was directly enabled by the integrating non-kinetic cyber capabilities with traditional force application approaches.

Military Operational Design

Operational design elements 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.[9] The generalized set of effects cyber weapons seek (knowledge of adversary presence in and use of cyberspace, assurance of friendly systems and ability to operate in and shape cyberspace, and military operational advantage in cyberspace) are the informational conditions necessary for achieving military 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 have yet to be observed in a showdown force-on-force, peer-competitor environment. We have only isolated, largely un-integrated examples and hints, and our own progress in developing organizations, processes, and tools for a grand information strategy is nascent. It is, however, the information-based activities resident in the cyber domain that are undoubtedly growing in significance both relative to other war fighting domains, and as a distinct class of war fighting capabilities.

Absent 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 future force and capabilities planning carry a degree of uncertainty and risk for the future. 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 is 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 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 those that ever more creatively employ the opportunities of cyberspace.

The Role of Technology

While there is widespread agreement that technology developments are fundamental to enabling new ways of operating in cyberspace, expert views diverge on whether technology is driving new operating concepts, or conversely, new concepts flow from the creative application 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 information advantage. 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 impacts of cyber capabilities. For example, while Lonsdale found that technological developments associated with the Information Revolution could have significant geopolitical and strategic impacts, he believed such developments would not drive information to predominate as an element of national power.[10] Dearth and Williamson similarly found that "ends" and "means" of war will change in the Information Age.[11] Cooper and Goure offered that technology fundamentally changed the way military forces are managed, integrated, and commanded in warfare, but war fighting strategy itself had not changed. Cooper also found that new non-

governmental entities would likely emerge as fundamental elements of the national security structure.[12]

Moving towards the opposite end of the spectrum, Brown found that new synergies in force application introduced through information technology advances do have the potential to revolutionize warfare, but ultimately, technological advantage itself would not guarantee success in war.[13] Vlahos found that emerging technology would enable, but not be the driver for, a fundamentally new social order characterized by revolutionary war -- a type of that America is both incapable of foreseeing and unable to control because of its great power status.[14] 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'."[15] The uncertainty that new cyber capabilities carry introduce risk for selecting new war fighting strategies and making related cyber resource investments. A common approach to evaluate and characterize the changes and impacts of operating in cyberspace is needed, and would greatly facilitate the formulation of new cyberspace operating concepts, as well as resource investments.

Principles and Functions of War

The Joint Doctrine for 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 electromagnetic 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. 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 formally referred to as "Military Operations Other Than War," these include restraint, perseverance, and legitimacy, and reflect a broader military role across the spectrum of peace and conflict, including specifically the missions of homeland security, stability operations, and flexible deterrent options.[16] This change also recognizes the growing prevalence of military operations outside of major combat scenarios, as well as the influence of globalization and its enablers in shaping the types of conflicts in which the U.S. engages. Activities in cyberspace related to these non-traditional 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 7 provides a mapping of potential application of cyber roles and capabilities that demonstrate each of the principles. Specific cyber capability descriptions are discussed in Chapter 5.

Table 7. 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 IPOE, Cyber attack to control or disable enemy systems
Offensive	Achieve military objective	Seize, retain, 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/C4ISR networks through layered defense,self-healing,robust reconfiguration
Economy of Force	Preserve capability to mass	Enable secondary missions	Defensive	Provide stand-alone non-kinetic 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/C4SIR networks through layered defense,self-healing,robust reconfiguration
Security	Enhance freedom of action	Reduce friendly vulnerability to hostile acts, influence, surprise	Defensive	Cyber defense and Cyber ISR
Surprise	Gain combat power advantage	Support rapid decision making, Deception, OPSEC	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 non-kinetic options
Perseverence	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

---

[1] Jeffrey R. Cooper, "Another View of Information Warfare," in *The Information Revolution and National Security Strategy*, ed. Stuart J. D. Schwartzstein (Washington, DC: The Center for Strategic and International Studies, 1996), 122.
[2] Stuart J. D. Schwartzstein, ed., *The Information Revolution and National Security* (Washington, DC: The Center for Strategic and International Studies, 1996), 37-180.
[3] Air Force Policy Directive 10-28, *Air Force Concept Development*, 15 September 2003.
[4] Air Force Policy Directive 10-28, 15 September 2003.
[5] Carl von Clausewitz, *On War*, Eds. and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 117-118.
[6] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Kings College, 2004), 216-217.
[7] Sun Tzu, *Art of War*, translated by Lionel Guiles, 1910. Accessed on line at http://etext.library.adelaide.edu.au/mirror/classics.mit.edu/Tzu/artwar.html, 28 Oct 2006.
[8] John F. Schmidt, *A Practical Guide for Developing and Writing Military Concepts*, Defense Adaptive Red Team Working Paper #02-4 (McLean VA: Hick $ Associates, Inc., December 2002), 14-15.
[9] Joint Publication 3-0, Joint Operations, 17 September 2006, IV-8.
[10] Lonsdale, *Nature of War*, 180.
[11] Douglas H. Dearth and Charles A. Williamson, "Information Age/Information War," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Alan D. Campen et al. (Fairfax, VA: AFCEA International Press, May 1996), 26-28.
[12] Cooper, *Another View*, 124, and Daniel Goure, "The Impact of the Information Revolution on Strategy and Doctrine," in *Information Revolution and National Security*, ed. Stuart J. D. Schwartzstein (Washington, DC: The Center for Strategic and International Studies, 1996), 220.
[13] Michael L. Brown, "The Revolution in Military Affairs: The Information Dimension," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Alan D. Campen et al. (Fairfax, VA: AFCEA International Press, May 1996), 34-42.
[14] Michael Vlahos, "The War after Byte City," in *Information Revolution and National Security*, ed. Stuart J. D. Schwartzstein (Washington, DC: The Center for Strategic and International Studies, 1996), 100-106.

[15] Davis S. Alberts, *The Unintended Consequences of Information Age Technologies* (Washington, DC: National Defense University), 21-22.
[16] Joint Publication 3-0 (JP 3-0), Joint Operations, 17 September 2006, II-2.

Chapter 5

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 later 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."

Lieutenant General Michael Short, CFACC, Operation Allied Force

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

Lt Gen Elder, Commander, 8th Air Force and Commander, AFCYBERCOM

Air Force cyberspace operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects in cyberspace in support of combatant commander objectives. Cyberspace operations are only possible given appropriately trained personnel, 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 intelligence, surveillance, and reconnaissance (ISR) functions. Cyberspace in this context includes any devices that are assigned internet protocol (IP) addresses and comprise the global grid, such as internetwork-connected computers, supervisory control and data acquisition (SCADA) systems, Joint Tactical Radio System (JTRS) and other IP-based radio systems, and other IP-based devices. Cyberspace capabilities must be fully coordinated with capabilities offered in other war fighting domains.[1]

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 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 are 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 non-attribution not possible in other domains. Most importantly, these effects are not subject to the same sorts of international political consequences as 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 (EMMD).[2] 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 to manipulate 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 foment mistrust and divisions amongst his supporters under the right conditions. As mentioned in the previous paragraph, one of the strengths of cyber 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 on the span of effects, cyber brings new meaning to the term precision. The precision inherent in cyber attacks goes far beyond the ability to address specific targets; cyber is capable of 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 their 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 delaying or even stopping and invasion by remotely immobilizing the lead tanks of a force on a bridge, thwarting the passage of other forces.

Stealthy/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. While cyber activities are characteristically stealthy and difficult to detect, care must still be taken to ensure they are not discovered. Discovery risks loss of target access, adversary knowledge of cyber capabilities that may not be easily replicated or could be readily countered, and limitations of capabilities. Research should focus on reducing the requirement for stealth so that cyber can serve to provide better deterrent effects.

Non-attribution/Untraceable

The difficulty of detecting adversary cyber activities also makes them more challenging to trace and attribute. While these capabilities are embedded in some tools and methods, manual actions such as log manipulations are frequently required. These characteristics are 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 impacts when cyber capabilities are employed. In this way they also can be used to aid other elements of national power rather than hinder them.

Cyber Capabilities

Cyberspace capabilities can be classified 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 non-kinetic domain have analogs in the kinetic domains.[3] However because operations in the cyberspace domain are virtual, the relative precedence of these capabilities is entirely different. For example, a greater premium is placed on stealth and low probability of detection than in many kinetic operations. This is because activities in the cyber domain are dependent on continued access to target systems and detection could result in loss of access due to disconnection or improved security measures. Conversely in the physical domains, some ISR activities such as mapping enemy territory can be carried out openly.

Cyber ISR

Cyber ISR (termed computer network exploitation in joint doctrine) is the cyber equivalent of kinetic intelligence preparation of the operational environment.[4] Successful cyber attacks and defenses require the comprehensive knowledge of own capabilities and system configurations, as well adversary systems and their configurations, provided by cyber ISR.

As mentioned above, cyberspace operations of all types are heavily dependent on sufficient information on the function, configuration, and criticality of adversary systems. The major functions of cyber ISR involve the following general steps also illustrated in figure 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.[5]
2. Access is obtained through direct adversary network penetration or through the installation of trapdoors, backdoors and multi-role, customizable mobile code called "cyber craft."
3. Data on the target system configuration is then ex-filtrated,
4. Analysis of the data is conducted, and
5. Ultimately an adversary target system model is created.[6]

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

The end goal is the accurate modeling of an adversary's systems by systematically and methodically mapping their 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 enumerating 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.[7]

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

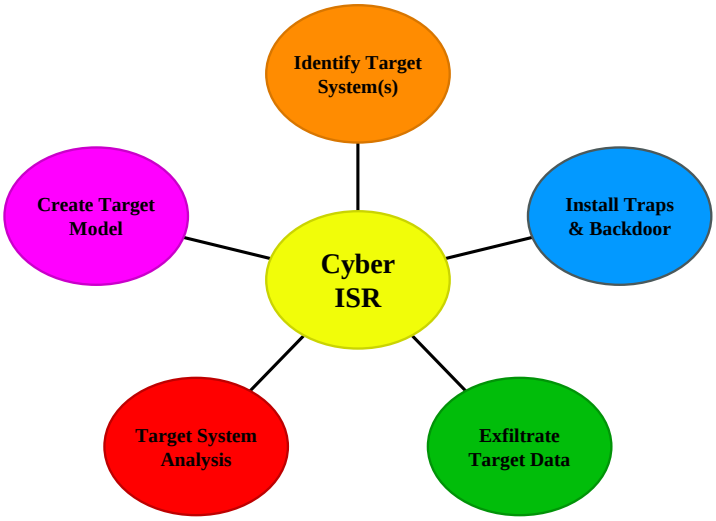

Figure 7. Principal Elements of Cyber ISR[8]

The borderless nature of cyberspace and the requirement to conduct adequate cyber ISR covertly and without attribution raises 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 and the need for a presidential finding before operations can begin and regular report to Congressional Intelligence Oversight Committees.[9] It is critical that these restrictions be resolved; otherwise, cyberspace operations will be hampered.

Target System Identification and Profiling

These are 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 its systems. Determination of the type (defensive or offensive) and intended scope of a particular cyberspace operation based on the desired effects is required prior to target identification and beginning cyber ISR in support of it. Only after the desired effects are fully understood should identification of adversary target systems begin. Existing all-source intelligence contains a wealth of information about potential adversaries that could be leveraged.

New target intelligence gathering efforts should be properly authorized, submitted and prioritized for collection as needed including "social engineering" activities involving human intelligence.[10] Types of information typically collected at this point include adversary organizational structure, publicly available personnel data, data archived on search engines, network security-related policy documents, former and disgruntled employees information, internet connectivity link providers, and public access web pages and other access sites. Internet domain name and IP address registration information can be obtained from the central internet registration authorities such as the Internet Corporation for Assigned Names and Numbers (ICANN) or subordinate regional registries.[11]

Once the needed general information is collected 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 to and from it.[12] Profiling in turn allows identification of the network protocols used and the addresses of machines performing certain functions on the target network, giving the clues about its topology. Reliable identification and profiling of the target is required as a starting point to perform the next step, scanning, access, privilege elevation, and permanent presence installation.

Access and Installation of a Persistent Presence

Regardless of whether it is obtained through social engineering, interception, or more direct methods, unauthorized access to adversary systems must be obtained in order conduct effective operations. The end goals of this stage are to map all possible avenues to approach the target, then 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, candidate systems should be remotely and discreetly swept

and scanned by active, passive, and fully automated techniques designed to determine what operating systems they are running and which services are available via its access points, also known as "ports."

Once these available ports and services are fully known, the next task is to determine which of these offers the possibility of basic access. This process is called "enumeration."[13] An ever expanding variety of methods to effect enumeration and determine the operating systems, applications, and network protocols used are possible while remaining anonymous and undetected. A partial list is given below:

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 "Cybercraft" designed to collect information
8. Proliferating worms, viruses and other mobile code designed to grant access[14]

Since anonymity and deniability are essential elements of cyber operations, methods such as network address spoofing are employed in the phase.[15] Care should also be taken to ensure that the intensity of operations (network traffic) does not rise to a level that would easily be detected through the use of slow scanning and judicious use of other tools and techniques.

Mapping of Enemy Systems and Data

Once continual access is guaranteed and administrative control assured, the focus of cyber ISR is to use 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.[16] 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 is the use of remote applications that can operate through backdoors installed during earlier access attempts. Remote control of machines on the adversary’s network offer access to a wealth of system information particularly when coupled with elevated system administrator privileges.[17] Remote control capabilities can be implemented 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 is called “port redirection” and is typically used to circumvent network security devices such as firewalls.[18]

After large amounts of data and control over adversary Internet, Intranet, Extranet, and Remote Access network and computing resources are obtained, mapping can be completed. A completed map should include information about both the internal and external systems that comprise the adversary 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 hardware firmware versions. A comprehensive map greatly improves the likelihood of accurately determining adversary capabilities and intent.

Analyzing Adversary Capabilities

A solid technical map of how the adversary's cyber systems function is not sufficient to fully understand their capabilities however. While it is obvious what part some systems such as firewalls play in the overall scheme of an adversary network, some are so generic that it is not clear what purpose they serve. They may even serve many purposes simultaneously or at different times depending on the software loaded and the hardware attached or embedded. Further traffic monitoring is required to determine their typical primary and ancillary functions.

Depending upon the extent that adversary 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 the various devices on the network. Generally however this is a manual process because many actions can be characterized as defensive, offensive or simply routine maintenance. Final characterization of capabilities requires the attention of fully-trained network infrastructure and applications program experts schooled in network defense and offense. Taken together, profiled traffic and adversary system maintenance, defense, and even attack exercises and methods reveal the full gamut of adversary capabilities.

Determining Adversary Intentions

Determining adversary intentions can be extremely difficult even after their technical capabilities are fully known and behaviors have been fully documented. However, the existence of servers and other devices on the target network observed to be 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 are important indicators of offensive intent. Other indicators can be obtained through an exhaustive search of the materials exfiltrated

from the target network. Specific evidence of intent include coordination procedures for offensive operations, actual targeting plans or lists, administrator chat sessions discussing such events, and manuals for executing attacks. While all these factors are important in determining the adversary's defensive or offensive intent, they are even more important as indications and warning (I&W) of impending attack.

Attack/Retaliatory Strike Planning

Cyber ISR is essential to successful prosecution of any cyber attack or defensive retaliatory strike. The research and analysis required in order to be successful is extensive and was thoroughly outlined in earlier parts of this section. No offensive or retaliatory actions should be undertaken until adequate cyber ISR is conducted and the proper authorization to perform attacks is obtained.[19] In the interim and because of the breath and depth of analysis required, it may be necessary to perform an array of defensive measures until adequate preparations for offensive operations are made and can be executed.

Cyber Defense

Communications are an essential element of every aspect of Western society and impact the functions of every element of national power, including military power. Defense of those capabilities is critical to the national survival of those societies and nations. Cyber defense consists of the protection, detection and attribution of computer network attacks and the reconstitution and recovery of friendly information systems after an attack from adversary attempts to destroy, disrupt, corrupt, or usurp them.[20] Attacks on our national and military information infrastructure are multi-dimensional and constantly increasing in frequency and scope. Due to the open distribution of automated tools for hacking on the Internet, the

knowledge required to execute increasingly sophisticated attacks has declined significantly as illustrated in figure 5.

Friendly forces must employ coordinated, defense in depth capabilities to anticipate and preempt adversary attacks on our information systems.[21] When adversary computer and network attacks are successful, information defense must rapidly minimize their effects and develop COAs to respond and prevent recurrence.

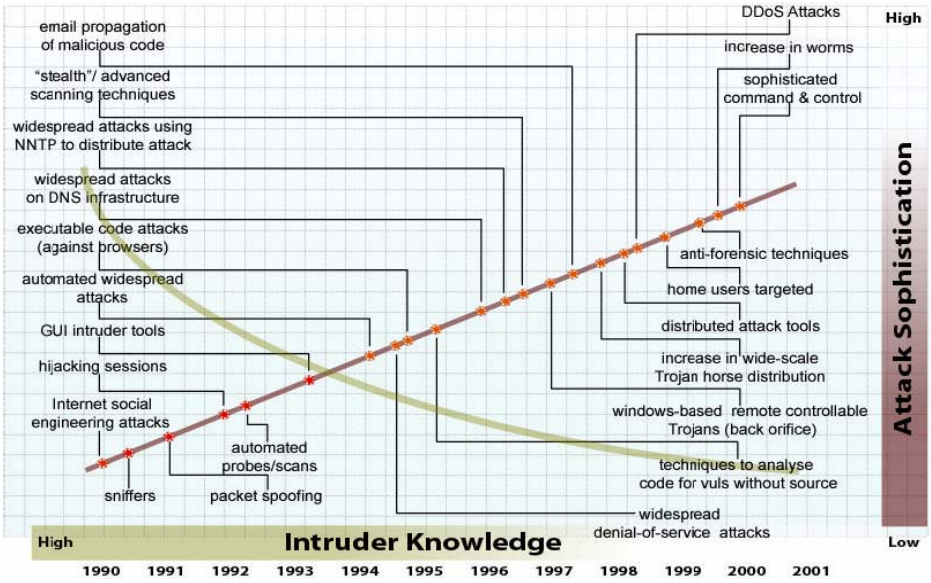

Figure 8. Cyber Attack Trends[22]

© 1998-2003 by Carnegie Mellon University

Friendly cyber defense will anticipate and defeat a wide array of persistent and simultaneous attacks. In addition to defense 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. 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, and certification and accreditations of new systems. Assessment includes both "gray" (cooperative) and "red" (covert) system tests by friendly security experts.[23] For example, Operation Eligible Receiver, a "red hat" exercise, was conducted in 1997 and 2003 to assess DoD system vulnerabilities through actual hacking and scanning.[24] The DoD concept of defense in depth involves protection at four layers: network and infrastructure, enclave boundaries, the 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.[25]

Protection from Attack

Indications and warnings derived from properly conducted cyber ISR is the best protection against adversary attacks. Firewalls and router access control measures are the principle direct means used to protect networks from attack. Other methods can be employed however to robust these basic structures.

Other methods of protection include redirection of attacks via packet forwarding or attracting hackers to artificially created environments called "honeynets" where they can be effectively monitored, controlled, and identified without making them aware.[26]

Attack Detection and Attribution

Attacks can come in many forms as shown in Table 8, but standard intrusion detection systems are employed at every echelon of Air Force networking to ensure attacks are detected.[27] Honeynet environments and system management "traps" that generate alarms when certain critical management actions are performed can also aid in detection of attacks.

Table 8. Classes of Attack[28]

Attack	Description
Passive	Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capture of 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 type individuals 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 into a product, such as a back door to gain unauthorized access to information or a system function at a later date.

Honeynets can also be employed to attribute attacks despite attacker attempts to hide their identities via IP spoofing. Honeynets can produce direct technical information about the attacker and keep attackers "on the line" long enough to be traced.[29] New methods are also being developed to attribute attacks based on the software they leave behind or the methods they used including the Hacker Profiling Project (HPP) at the United Nations Interregional Crime and

Justice Research Institute (UNICRI). Indications and warning from cyber ISR, however remain the best and most reliable method of attribution.

Automated Attack Responses and Operator Alerts

A variety of new network protection systems are capable of detecting and providing a limited automated protective response to attacks.[30] Linking detection to automated responses, automated operator alerts, and alarms are key to ensuring that defense remains viable as the volume of network traffic increases. Care must be taken to ensure that these automated responses cannot be manipulated by attackers or result in self-imposed denial of service attacks and impact to operations.

Self-healing of Systems and Networks

Self-healing is a fourth generation networking capability beginning to appear in commercially available systems and is highly desirable in environments that require high assurance computing and networks.[31] Networks have long possessed limited abilities to re-route 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, it is critically important that this capability is high assurance, otherwise it could be manipulated by attackers.

Rapid Recovery after Attack

Backup systems have been the primary element in data disaster and attack recovery for many years. However, fast, 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 automated system features, namely that the risk that system could be manipulated by attackers or suffer a malfunction.[32]

Cyber Attack

There are a large array of existing technical capabilities that can be used to conduct offensive operations in cyberspace against adversary data, systems, and networks in support of combatant commander objectives. In addition to certain special technical operations (STO) capabilities already in existence, research and development is constantly producing more options. New, more flexible capabilities such as "cybercraft" that can serve cyber ISR, defense, and offense purposes are under development to ensure our capabilities keep pace with ever changing threats and defenses.[33]

"Commercially available" attack methods can also be used as a model to augment designs for new capabilities. Some of these capabilities are outlined in the Table 9, in order of increasing sophistication required to execute them.

This list, while not exhaustive, covers the major categories of attack and describes their most common methods of execution. While the vulnerabilities they exploit and the design concepts they use can be applied to enhance designs, care should be taken not to use the actual code without thorough investigation.[34] Regardless of whether the capability was developed by commercial or government sources, all attacks and methods of access are highly perishable once revealed.

Table 9. Common Cyber Attack Categories and Methods[35]

Attack	Description
Denial Of Service (DoS) Attacks	
Flooding	Sending extraneous data or replies to block a host services
SYN/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 DoS	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-less services
Nameserver ID "Snoofing"	Blind spoofing with calculated false ID numbers NS-caches
Sequence Number Guessing	Calculating TCP SEQ/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	Replace system files with trojans to hide unauthorized access
Sniffing	Monitor network data to find sensitive data e.g. passwords
Non-Blind Spoofing	Monitor network to hijack active or make forged connections

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 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.[36] Chapter 7 will explain the measures that should be taken to improve leadership confidence in these capabilities and allow for their effective employment.

Disruption of Adversary C2 Systems, Processes, and Data

The capability to temporarily disrupt the operation of adversary command and control (C2) systems is a key element of cyber attack. The categories of attack typically employed to disrupt systems involve exploiting vulnerabilities or malicious software.[37] System disruptions are effective for two principal reasons: first, the interruptions can be triggered to occur at a time and place of our choosing and 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 Adversary Systems and Data

Denying access to adversary systems without destroying 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.[38] While execution of these types of attacks can be controlled, network defenses will likely prevent their reapplication and result in the loss of the access to the adversaries systems. Therefore,

careful consideration of the benefits and costs of execution should be taken into account prior to undertaking cyber denial.

Degrading Adversary System Performance

Degrading adversary cyber capabilities is essentially a less extreme form of cyber disruption. Slowing or intermittent access to applications or networks can effectively distract the adversary and slow their decisions cycles. Unlike in cyber disruption however, adversary system personnel retain access to their systems and can monitor system performance in real time potentially exposing friendly efforts at cyber degradation. If cyber 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 system.

Destruction of Adversary Data, Computers, Networks

Destruction of a part of an adversary's cyber capabilities has both advantages and disadvantages. The 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 the threats their 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 adversary networks.

Cyberspace Effects

Combatant Commanders will employ Air Force cyberspace operations pre-conflict, during conflict, and post-conflict in order to achieve desired effects as a part of a larger joint operation. Air Force Cyberspace Operations will be conducted as a 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, DoD Directive

3600.1, joint guidance found in Joint Publication 3-13, Air Force Doctrine Document 2-5, and the legal restrictions outlined in the DoD Information Operations Roadmap.[39] In addition to pointing out the need to resolve doctrinal and legal issues, the DoD IO 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 post-conflict stages, its activities can act as supported or supporting military courses of action.[40]

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, cyber should be supported by other, more traditional options, to include kinetic ones. Friendly forces in cyberspace consist of software and inexpensive hardware that are designed to be easily reconstituted and no operators are placed at physical risk. Depending on the adversary systems targeted and the manner in which the impacted, the resulting physical damage can be controlled by the attacker. Some cyberspace options are so unique to the medium that they are not otherwise 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 through a variety of capabilities. In fact, some Air Force cyberspace options can allow the military to contribute more directly to the effects of non-military elements of power such as the diplomatic, informational, or economic by holding adversary cyber assets at risk.

Foresight in diplomatic affairs can be a crucial advantage. Capabilities such as electronic eavesdropping to predict adversary initiatives, intercepting and manipulating or delaying

diplomatic messages, and electronic manipulation of adversary intelligence can provide friendly diplomatic corps an unbeatable edge. The ability to know what the adversary will propose and what their 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 are nearly boundless. Internet site manipulation and interception and manipulation of enemy internet and radio-based command and control could be particularly useful in producing information effects needed to combat terrorism. In more traditional conflicts with nation states, cyber could be used to negatively impact adversary 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 impacting 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 ISR

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 organizations 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 effects 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 non-repudiation. The value of these aspects of information assurance 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 friendly counter strikes are properly directed. The most important potential effect of a strong cyber defense is to make cyber attack upon friendly forces seem 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 indirectly effect 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 the fact that they use is apparent and easily countered once used. 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.

---

[1] *Air Force Concept of Operations for Information Operations* (AF IO CONOPS), 6 February 2004, 3.
[2] William J. Bayles, Parameters, "The Ethics of Computer Network Attack", Spring 2001, 44-58.
[3] Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (JV 2020), June 2000, 8-10, 22, 23.
[4] Joint Publication 3-13, Information Operations, 13 February 06, GL-6.
[5] Kevin D. Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis, ID: Wiley Publishing, Inc., 2002), 31.
[6] Dr Paul W. Phister, et al, *CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment*, AFRL Information Directorate, (Rome, NY: Air Force research Laboratory, 23 February 2006), 5-6.
[7] Stuart McClure, Joel Scrambray, and George Kurtz. *Hacking Exposed Fifth Edition: Network Security Secrets and Solutions* (Emeryville, CA: McGraw Hill/Osborne, 2005), 7.
[8] Col Sparks, "67 Network Warfare Wing Mission Brief"" (lecture, Air Intelligence Agency (AIA), Kelly AFB, TX, 4 September 2006.)
[9] International and Operational Law Department, The Judge Advocate General's Legal Center and School, *Army Operational Law Handbook 2002*, Chapter 20, "Information Operations," 3.
[10] Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: 'The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (Indianapolis, ID: Wiley Publishing, Inc., 2005), 62.
[11] Stuart McClure, Joel Scrambray, and George Kurtz, *Hacking Exposed Fifth Edition: Network Security Secrets and Solutions* (Emeryville, CA: McGraw Hill/Osborne, 2005), 19.
[12] Donald L. Pipkin, *Halting the Hacker: A Practical Guide to Computer Security Second Edition* (Upper Saddle River, NJ: Prentice Hall PTR, Inc., 2003), 174.
[13] Stuart McClure, Joel Scrambray, and George Kurtz, *Hacking Exposed Fifth Edition: Network Security Secrets and Solutions* (Emeryville, CA: McGraw Hill/Osborne, 2005), 78.
[14] John Chirillo, *Hack Attacks Revealed*: *A Complete Reference With Custom Security Hacking Toolkit* (New York, NY: John Wiley & Sons, 2001), 45.
[15] Stuart McClure, Joel Scrambray, and George Kurtz, *Hacking Exposed Fifth Edition: Network Security Secrets and Solutions* (Emeryville, CA: McGraw Hill/Osborne, 2005), 186.
[16] Ibid, 175.
[17] Ibid, 189.
[18] Ibid, 190.
[19] International Relations Research Center (IRRC), "Wired warfare: Computer network attack and jus in bello," *IRRC Review* 84, no. 846 (June 2002): 396-398.
[20] *Air Force Concept of Operations for Information Operations* (AF IO CONOPS), 6 February 2004, 14.
[21] Leigh Armistead, Information Operations : Warfare and the Hard Reality of Soft Power (Washington, DC: Brassey's, Inc., 2004), 84.
[22] Carnegie Mellon CERT Coordination Center, "Incident and Vulnerability Trends, 2003", 18.
[23] 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.
[24] Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (Indianapolis, ID: Wiley Publishing, Inc., 2005), 41.
[25] Information Assurance Technical Forum, *Defense in Depth.* (Washington, DC: Government Printing Office, 2002), 7.
[26] The Honeynet Project, *Know your Enemy: Learning About Security Threats (Second Edition)* (New York, NY: Addison-Wesley Professional, Inc., 2004), 40.

[27] Kelvin Wong, Swinburne Review, "Implementing Security: Introduction to Hacking Methods and Ways of Counter-Measure," Winter 2005, 9.
[28] Information Assurance Technical Forum, *Defense in Depth.* (Washington, DC: Government Printing Office, 2002), 5.
[29] The Honeynet Project, *Know your Enemy: Learning About Security Threats (Second Edition)* (New York, NY: Addison-Wesley Professional, Inc., 2004), 50.
[30] Joseph Giordano, "Cyber Operations: A Historical Perspective" (lecture, AFRL Rome Research Site (RRS), Rome, NY, 14 September 2006.)
[31] Ibid, 4.
[32] Ibid, 4.
[33] Dr Paul W. Phister, et al, *CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment*, AFRL Information Directorate, (Rome, NY: Air Force research Laboratory, 23 February 2006), 8.
[34] Hugo Cornwall, *Hacker's Handbook* (Philadelphia, PA: E. A. Brown Co., 1986), 10.
[35] Ankit Fadia, *Network Security: A Hackers Perspective* (Cincinnati, OH: Premier Press, 2003), 165-230.
[36] International Relations Research Center (IRRC), "Wired warfare: Computer network attack and jus in bello," *IRRC Review* 84, no. 846 (June 2002): 396-398.
[37] Kevin D. Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (Indianapolis, ID: Wiley Publishing, Inc., 2005), 76.
[38] Rose Gr@ve, "A SYN-ful Experiment," 2600.com, 22 August 2005, http://www.2600.com/code/222/.
[39] DoD Information Operation Roadmap (IO Roadmap), 30 October 2003, 2.
[40] 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: Air University Press, December 2005), 19.

Chapter 6

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 U.S. 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 provided a synopsis of several critical factors and observations regarding the current cyber state of affairs. Each chapter puts 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 chapter will address these issues by advocating a holistic methodology to develop AF cyberspace mission capabilities, and 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 HP CEO
> *Tough Choices*

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 warfighting 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 U.S. 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.

Cyberspace and the Revolution in Military Affairs Debate

> *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*

The phrase "revolution in military affairs" (RMA) 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 revolution in military affairs gained prominence. Theorists debate net-centric warfare, information technology, the rise of asymmetric threats, information warfare, and now cyberspace as potential revolutions in military affairs.

Why spend any time discussing RMA and the 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 AF mission statement and to frame the methodology to achieve those outcomes. According to the Office of the Secretary of Defense, Office of Net Assessment:

> A Revolution in Military Affairs 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.

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, it 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 RMA, each with a slightly different slant on the definition. Some authors went so far as to subdivide their definition of a revolution in military affairs into "lesser" and "greater" RMA categories. Other scholars debate RMA with regard to the definition of "war" versus "warfare". Some scholars claim there have been ten revolutions in military affairs,

others assert three broad periods of revolution and still others stress specific technical innovations as revolutionary. Table 10 highlights some events that scholars consider RMAs.

Table 10. Survey of Suggested RMAs

Suggested RMAs

- Assyrian combined arms tactics
- Cavalry stirrups
- Persian and Byzantine heavy cavalry
- Infantry pikes and longbows
- Gunpowder
- Cannon
- Ship-borne cannon
- French military reforms of 16th 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 armour
- Medical revolution
- Indirect fire and the deep battle
- Submarine warfare
- Mechanised warfare in the 1930s and 1940s
- Blitzkrieg, strategic bombing, offensive carrier aviation, amphibious warfare
- Nuclear weapons and ballistic missiles
- Peoples' 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 RMA are listed in Table 11.

Table 11. Five Prominent Definitions for RMA

Definition	***Source***
RMA involves a paradigm shift in the nature and conduct of military operations which 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.	Krepinevich
A radical change in the conduct and character of war.	Gray
A discontinuous increase in military capability and effectiveness arising from simultaneous and mutually supportive change in technology, systems, operational methods, and military organizations.	Metz and 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.	Benbow

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

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 tends to be recognized as a principal source of RMAs, it is not necessary nor sufficient to an RMA.[1] Similarly, most scholars agree that RMAs are not accidental. RMAs 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 does 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 nor 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.[2]

Pushing aside the idea that cyberspace will revolutionize warfare allows the AF 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."[3]

Although not evident at the publishing of the new AF mission statement, it is now clear that the AF does not regard cyberspace as an RMA but rather as "a domain where the Air Force conducts operations."[4] This distinction is significant. As was illustrated in Chapter 4 of this paper, cyber capabilities <u>support</u> the principles of war, they do not change them. The cyber domain is simply another place to operate. How the AF harnesses the power of cyberspace in support of U.S. national interests will be determined, in large measure, by the methodology it employs to define its role in the cyber domain.

Cyberspace Operations as a Mission Capability Package

> *Exposure to new information technologies and their capabilities is potentially dangerous unless it is accompanied by changes in a number of key dimensions. Further, 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*

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 U.S. 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 AF must steer clear of returning to its *querencia.*

Effectively flying and fighting in cyberspace requires 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 Department of Defense. The process is called the "mission capability package" developed by the Command and Control Research Program.

The Command and Control Research Program (CCRP) was initiated in the 1990s through a recommendation by the Defense Science Board in response to the need to better understand command and control. Over the years, this organization evolved and expanded. Today, CCRP resides under the Deputy Assistant Secretary of Defense (NII) 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.[5] One of the key concepts developed by this program is the Mission Capability Package concept.

The Mission Capability Package (MCP) concept is 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, stay away from the AF *querencia*. The approach CCRP developed to build a mission capability package should be used by the Air Force to exploit the power of cyberspace in support of U.S. 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, the 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 an MCP approach to co-evolve the way it organizes, trains, equips, and fights with portions of its force. Figure 6 depicts the mission capability package development process.

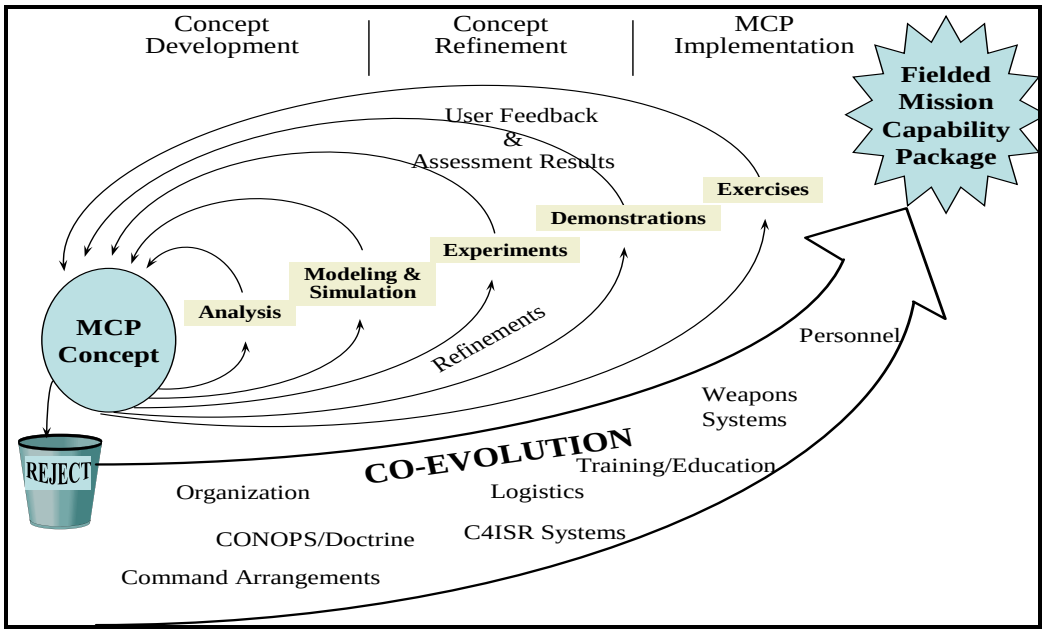

Figure 9. Mission Capability Package Process

Source: David Alberts. *Information Age Transformation: Getting to a 21st Century Military*. Library of Congress, Washington, DC, March 2003, 76.

The MCP process will assist the Air Force in understanding the implications of emerging cyber technologies and to concurrently develop the necessary changes in other areas ensuring a holistic approach. As the AF 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*

In as much as 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 Air Force is not yet postured to

fulfill this mission.[6] Forming policy and changing mission statements is 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.[7] 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 is ahead for the Air Force as it simultaneously lays claim to a role as lead Service within 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 cyber power. It can no longer view cyber power solely as an adjunct to air power 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 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."[8]

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 compromised of commonly available hardware and networks. In contrast, the other two mission areas conducted within the EM, electronic warfare and directed energy, require both uniquely specialized hardware and skills. Development of all these skills should be inserted within the top ten priorities on the Air Force network defense requirements priority list.

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 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 called "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 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.[9] 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 they need to be effective.

Training for Cyber Combat

As mentioned in the previous paragraph, it is not enough to simply 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 such service obligations for those whose education and training is 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 sub-parts 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. 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 only be possible 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, adequate and focused cyber training has to be administered. That will require the creation of a raft of specialty cyber training classes and the instructional corps to administer the classes. Much of the training could be conducted virtually of course, but the nature of cyber operations may require other types of non-technical 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 sub-categories of training required align with the three principal missions conducted in the EM environment: network warfare, electronic warfare, 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 between them.

The acquisition of talent and training should be carefully articulated by AFCYBER Command. However, recruiting, education, and training alone are not enough to ensure success. A professional core of cyber professionals that 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 air power theory and "air mindedness," the establishment of a cyber command is an important step in developing cyber power. The US Army Air Corps provided the sort of "immersion" in air thinking needed for theories of air power 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 Air Staff, the cyber "Go Do" Letter,[10] designates the 8th Air Force Commander as the Commander, Air Force Cyber Command.

Below the command level however, the cyber command will need to be organized in ways to which the Air Force is not accustomed in order to be effective. Cyber warriors operate in an environment that is 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.[11] 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 the 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 non-traditional, will serve to institutionalize cyber-mindedness within the Air Force and improve its effectiveness.

The cyber command will provide a way for the Air Force to streamline presentation of cyber forces to USSTRATCOM 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 the new cyber command have several geographically-separated operating locations both to protect its capabilities and enhance the diversity of options developed.

Cyber Weapon Funding

Dedicated funding for professional research and design of cyber weapons and payloads are critical to delivering the options needed by the combatant commanders. According to a famous quote by Brig Gen William “Billy” Mitchell, the first essential of air power 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 is 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 Air Force must fund, build, and maintain a distributed capability to rapidly generate and integrate new cyber attack weapons, and just as rapidly counter new adversary 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 AIA, Rome Laboratories, AFC2ISR, and other Air Force units worldwide. Rough investment estimates to jumpstart cyber capabilities for the first five years of AFCYBERCOM total approximately $620 million, with fully one third of that amount going to cyber recruitment and training.

Air Force Material Command is already engaged in a major research effort at its Rome Research Site to acquire "cyber craft," a cyber analog to aircraft (see Figure 10), but the effort is dire need of additional funding.[12] The goal of this research is to create small, mobile, and highly autonomous programs capable of carrying out ISR, defensive and offensive cyber activities, and 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.

Figure 10. Kinetic Air and Space vs. Cyber Craft Comparison[13]

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, AFCYBERCOM should be empowered by the Congress to budget separately to organize, train, and equip in a way similar to U.S. Special Forces Command. This will ensure that existing Air Force programs are not adversely impacted by the increased funding demands of developing cyber capabilities.

Air Force research and design efforts 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.[14] Sharing and de-confliction of research efforts would conserve every agency's funds and answer critics such as the General Accounting Office.[15]

It is only through full and rigorous development that combatant commander 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 cyber capabilities usage as weapons under the Geneva Conventions remains unclear.[16] If the status is not resolved, combatant commanders will continue to avoid the application of cyber options.[17] This is clearly a subject that requires further consideration. In the absence of definitive international guidelines, clear and specific directives that delegates the authority to use cyber options to combatant commanders and other U.S. government agencies is critical to enabling the application of cyber power.

---

[1] Tim Benbow, *The Magic Bullet? Understanding the Revolution in Military Affairs*. London, Chrysalis Books Group, Brassey's Publishing, 2004, 19.
[2] Ibid, 14.
[3] Colin Gray, "Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context." Strategic Studies Institute, February 2003: 49.
[4] Dr. Lani Kass, director of the Air Force Cyberspace Task Force, AFPN, April 2006.
[5] Department of Defense, Command and Control Research Program (CCRP), http://www.dodccrp.org/.
[6] Reuters, "Air Force Makes Bid for Mission in Cyberspace," *Google News*, 3 December 2005, http://www.google.com/.
[7] Dr. Lani Kass, Director CSAF Cyberspace Task Force, "Cyberspace, War Fighting Domain" (address Air Force Association Convention, Washington, DC, 26 Sep 2006).
[8] Michael W. Wynne, Secretary of the Air Force and Gen T. Michael Moseley, Chief of Staff of the United States Air Force to Commanders of ACC, AETC, AFMC, and AFSPC, Memorandum, "Establishment of an Operational Command for Cyberspace," 6 September 2006.
[9] Bill Gertz, "Chinese hackers prompt Navy college site closure," *Washingtontimes.com*, 30 November 2006, http://washingtontimes.com/national/20061130-103049-5042r.htm.
[10] Gen T. Michael Moseley, Chief of Staff of the United States Air Force to Lt Gen Robert J. Elder, Commander, 8th AF and AFCYBER, Memorandum, "Operational Cyberspace Command "Go Do" Letter," 2 November 2006.
[11] Dr. Lani Kass, "Cyberspace, War Fighting Domain" (address, Air Force Association Convention, Washington, DC, 26 September 2006).

[12] Dr. Paul W. Phister, et al, *CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment*, AFRL Information Directorate, 5-6.
[13] Dr. Kamal Jabbour, AFRL Rome Research Site (RRS), "RRS IF Directorate Mission Brief" (lecture, AFRL Rome Research Site (RRS), Rome, NY, 14 September 2006.)
[14] White House, *National Strategy to Secure Cyberspace*, 2003, 20.
[15] John Monroe, "Feds still lack security research agenda," *FCW.com*, 1 November 2006, http://www.fcw.com/article96662-11-01-06-Web&newsletter=yes.
[16] International Relations Research Center (IRRC), "Wired warfare: Computer network attack and jus in bello," *IRRC Review* 84, no. 846 (June 2002): 367.
[17] DoD Information Operation Roadmap (IO Roadmap), 30 Oct 2003, 2.

Chapter 7

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***"**

The quote above 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 those words meant. Nonetheless, 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 eradicates 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, this paper 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 to include 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 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 how data is knowable and usable 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 U.S. cyber situation. The Air Force must examine current cyber conditions, analyze cyber threats, dissect current vulnerabilities, and clearly define how and where the Air Force 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 only possible given 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 intelligence, surveillance, and reconnaissance (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 AF harnesses the power of cyberspace in support of U.S. 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 of 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 are 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. Per 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.[1]

[1] Schmitt, "*A Practical Guide for Developing and Writing Military Concepts,*" p. 22.

Bibliography

1. *Air Force Concept of Operations for Information Operations* (AF IO CONOPS), 6 Feb 2004.

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

3. Air Force Policy Directive 10-28. *Air Force Concept Development*, 15 September 2003.

4. Alberts, David S. *The Unintended Consequences of Information Age Technologies: Avoiding Pitfalls, Seizing the Initiative*. October 1996. Reprint, Washington, DC: National Defense University, 1996.

5. Alberts, David. *Information Age Transformation: Getting to a 21st Century Military*. Washington, DC: Library of Congress, March 2003.

6. Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, DC: Brassey's, Inc., 2004.

7. Bayles, William J. "The Ethics of Computer Network Attack." *Parameters* (Spring 2001): 44-58.

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

9. Bennett, John. "Air Force to Establish New Cyberspace Operations Command." *World Politics Watch*, 4 Oct 2006. http://www.worldpoliticswatch.com/.

10. Billo, Charles and Welton Chang. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States.* Dartmouth College Institute for Security Technology Studies, December 2004.

11. Brown, Michael. "The Revolution in Military Affairs: The Information Dimension." In *Cyberwar: Security, Strategy and Conflict in the Information Age.* Edited by Alan D. Campen et al. Fairfax, VA: AFCEA International Press, May 1996.

12. Carnegie Mellon CERT Symposium, "Incident and Vulnerability Trends, 2003." Briefing. CERT Coordination Center, PA, 10 December 2006.

13. Carnegie Mellon Software Engineering Institute, CERT Coordination Center. http://www.cert.org/.

14. Cebrowski, A.K. *Military Transformation: A Strategic Approach*. Washington, DC: Department of Defense, Fall 2003.

15. Chirillo, John. *Hack Attacks Revealed*: *A Complete Reference With Custom Security Hacking Toolkit*. New York, NY: John Wiley & Sons, 2001.

16. Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

17. Clausewitz, Carl von. *On War*. Edited by Anatol Rapoport. Translation published by Routledge & Kegan Paul Ltd, 1908. Introduction and notes copyright by Penguin Books Ltd, 1968. 16th reprint. Penguin Group: London, 1988.

18. Congressional testimony of John A. Serabian, Jr., Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the U.S. Economy, February 23, 2000 at http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html.

19. Congressional testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004. http://www.fbi.gov/congress/congress04/lourdeau022404.htm.

20. Cooper, Jeffery. "Another View of Information Warfare," in *The Information Revolution and National Security Strategy*, ed. Stuart J. D. Schwartzstein. Washington, DC: The Center for Strategic and International Studies, 1996.

21. Cordesman, Anthony H. and Cordesman, Justin G. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.* Westport, CT: Praeger, 2002.

22. Cornwall, Hugo. *Hacker's Handbook.* Philadelphia, PA: E. A. Brown Co., 1986.

23. *Critical Infrastructure Protection: Defending the U.S. Homeland.* Westport, CT: Praeger, 2002.

24. Cronin, Patrick M., Ed. *2015: Power and Progress*. Washington, DC: National Defense University, July 1996.

25. Darley, William M. "Clausewitz's Theory of War and Information Operations." *Joint Forces Quarterly*, issue 40 (1st quarter 2006): 73-79.

26. Dearth, Douglas H. and Charles A. Williamson. "Information Age/Information War," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Alan D. Campen et al. Fairfax, VA: AFCEA International Press, May 1996.

27. *Defense in Depth.* IATF Report. Washington, DC: Information Assurance Technical Forum, 2002.

28. DeMattei, Lou Anne. "Information Operations Doctrine: Service Perspectives." Research paper. Norfolk, VA: Joint Forces Staff College, April 2004.

29. Department of Defense Directive 3600.1 (Draft Version). *Information Operations*, October 2001.

30. Department of Defense Directive O-3600.1. *Information Operations*, 14 August 2006.

31. Department of Defense, Office of Force Transformation. http://www.oft.osd.mil/library/library.cfm?libcol=2.

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

33. Department of the Air Force. "Air Force Mission." http://www.af.mil/welcome.asp (accessed 25 Sep 2006).

34. DoD Information Operations Roadmap (IO Roadmap). 30 October 2003.

35. Fadia, Ankit. *Network Security: A Hackers Perspective.* Cincinnati, OH: Premier Press, 2003.

36. Farmer, David 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.

37. Federal Bureau of Investigation, National White Collar Crime Center. *IC3 2005 Internet Crime Report, January 1, 2005 – December 31, 2005*. Washington, DC.

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

39. Gertz, Bill. "Chinese hackers prompt Navy college site closure." *Washingtontimes.com*, 30 November 2006. http://washingtontimes.com/national/20061130-103049-5042r.htm.

40. Giordano, Joseph. "Cyber Operations: A Historical Perspective." Lecture. AFRL Rome Research Site (RRS), Rome, NY, 14 September 2006.

41. Goure, Daniel. "The Impact of the Information Revolution on Strategy and Doctrine," in *Information Revolution and National Security*, ed. Stuart J. D. Schwartzstein. Washington, DC: The Center for Strategic and International Studies, 1996.

42. Gr@ve, Rose. "A SYN-ful Experiment." *2600.com*, 22 August 2005. http://www.2600.com/code/222/.

43. Gray, Colin. "Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context." Carlisle, PA: Strategic Studies Institute, February 2003.

44. Gray, Colin. *Modern Strategy*. Oxford: Oxford University Press, 1999.

45. Hildreth, Steven. Congressional Research Service. *Cyberwarfare*, CRS Report for Congress. Washington, DC: Government Printing Office, June 2001.

46. *Homeland Security Act of 2002 and E-Government Act of 2002: Federal Information Security Management Act (FISMA).* 108th Congress, First Session, HR 2458, 7 January 2003.

47. Honeynet Project, *Know your Enemy: Learning About Security Threats (Second Edition).* New York, NY: Addison-Wesley Professional, Inc., 2004.

48. Interagency Working Group on Cyber Security and Information Assurance. *Federal Plan for Cyber Security and Information Assurance Research and Development*. Washington, DC: National Science and Technology Council, April 2006.

49. International and Operational Law Department, The Judge Advocate General's Legal Center and School, *Army Operational Law Handbook 2002*. Chapter 20, "Information Operations," 2003.

50. International Relations Research Center (IRRC). "Wired warfare: Computer network attack and jus in bello." IRRC Review 84, no. 846 (June 2002): [396-398].

51. Jabbour, Dr. Kamal. "RRS IF Directorate Mission Brief." Lecture. AFRL Rome Research Site (RRS), Rome, NY, 14 September 2006.

52. Joint Publication (JP 5-00.1). *Joint Doctrine for Campaign Planning*, 25 Jan 02.

53. Joint Publication 1 (JP 1-0). *Joint Warfare of the Armed forces of the United States*, 14 November 2000.

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

55. Joint Publication 3-13 (JP 3-13). *Information Operations*, 13 February 2006.

56. Joint Publication 3-13 (JP 3-13). *Information Operations* (second draft), 14 December 2004.

57. Kass, Dr. Lani. "Cyberspace: A War fighting Domain." Address. Air Force Association Air & Space Conference 2006, Washington, DC, 26 September 2006. www.afa.org/media/scripts/ppt_pdf/AFACyberspaceTaskForceBrief.pdf.

58. Kenyon, Henry S. "Networked Vision Moves Closer to Reality." *SIGNAL*, July 2004, 35-38.

59. Krepinevich, Andrew. "Cavalry to Computer: The Pattern of Military Revolutions." *The National Interest*, No. 37, Fall 1994.

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

61. Libicki, Martin C. *Defending Cyberspace and Other Metaphors*. Washington, DC: National Defense University, February 1997.

62. Lipsey, Lt Col Richard A. "Network Warfare Operations: Unleashing the Potential." In *Netted Bugs and Bombs - Implications for 2010*. Edited by Marsha J. Kwolek. Maxwell AFB, AL: Air University Press, December 2005.

63. Loescher, Michael S., et al. *Proteus: Insights from 2020*. Compiled by Pamela H. Krause. Washington, DC: The Copernicus Institute Press & Michael S. Loescher, 2000.

64. Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. Kings College London: London, 2004.

65. McClure, Stuart, Joel Scrambray, and George Kurtz. *Hacking Exposed Fifth Edition: Network Security Secrets and Solutions.* Emeryville, CA: McGraw Hill/Osborne, 2005.

66. Mitnick, Kevin D. and William L. Simon. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers.* Indianapolis, IN: Wiley Publishing, Inc., 2005.

67. Mitnick, Kevin D., and William L. Simon. *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, IN: Wiley Publishing, Inc., 2002.

68. Monroe, John. "Feds still lack security research agenda." *FCW.com*, 1 November 2006. http://www.fcw.com/article96662-11-01-06-Web&newsletter=yes.

69. Moseley, Gen T. Michael. Chief of Staff of the United States Air Force. To Lt Gen Robert J. Elder, Commander, 8th AF and AFCYBER. Memorandum, "Operational Cyberspace Command "Go Do" Letter," 2 November 2006.

70. National Security Agency. "What is Signals Intelligence?" http://www.nsa.gov/sigint/index.cfm (accessed 25 Sep 2006).

71. National Vulnerability Database. http://nvd.nist.gov/.

72. Office of Homeland Security. *National Strategy for Homeland Security.* Washington, DC: Government Printing Office, July 2002.

73. Office of Management and Budget, *FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, Washington, DC, 1 March 2006.

74. Office of the Manager, National Communications System. *Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications: An Awareness Document.* Arlington,VA, December 2000.

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

76. Pipkin, Donald L. *Halting the Hacker: A Practical Guide to Computer Security Second Edition.* Upper Saddle River, NJ: Prentice Hall PTR, Inc., 2003.

77. President Lincoln, "Second Annual Message to Congress, December 1, 1862. http://teachingamericanhistory.org/library/index.asp?document=1065.

78. President. *The National Security Strategy of the United States of America*. March 2006.

79. President. *The National Strategy to Secure Cyberspace*. February 2003.

80. President's Information Technology Advisory Committee. *Cyber Security: A Crisis of Prioritization: Report to the President*. National Coordination Office for Information Technology Research and Development, February 2005. http://www.nitrd.gov.

81. Reppert, Barton. "United States Facing Cyber Security Crisis, Experts Tell Capitol Hill Briefing, As IEEE-USA Prepares New Position Statement." *Today's Engineer Online*, August 2005. http://www.todaysengineer.org/2005/Aug/cybersecurity.asp.

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

83. Reuters. "Air Force Set to Fight in Cyberspace." *Google News*, 2 November 2006. http://www.google.com/.

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

85. Schmitt, John F. *A Practical Guide for Developing and Writing Military Concepts*. Defense Adaptive Red Team Working Paper #02-4. McLean, VA: Hick & Associates, Inc., December 2002.

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

87. Secretary of Defense. *Quadrennial Defense Review Report*. February 2006.

88. Secretary of the Air Force and Chief of Staff, US Air Force. To HQ ACC, HQ AETC, HQ AFMC, HQ AFSPC. Memorandum, 6 September 2006.

89. Secretary of the Air Force and Chief of Staff, USAF. To the airmen of the United States Air Force. Letter, 7 December 2005.

90. Steele, Robert D. *Information Operations: Putting the "I" Back into DIME*. Carlisle, PA: U.S. Army War College, 2006.

91. Stein, George J. "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.

92. Strange, Dr. Joe. "Understanding Centers of Gravity and Critical Vulnerabilities." Address. Air War College, Maxwell AFB AL, 28 November 2006.

93. Sparks, Col. "67 Network Warfare Wing Mission Brief." Lecture. Air Intelligence Agency (AIA), Kelly AFB, TX, 4 September 2006.

94. Tzu, Sun. *Art of War*. Audiobook translated by Lionel Giles, 1910; narrated by Scott Brick and Shelly Frasier, Tantor Media, January 2003.

95. Tzu, Sun. Art of War. Translated by Lionel Guiles, 1910. http://etext.library.adelaide.edu.au/mirror/classics.mit.edu/Tzu/artwar.html (accessed 28 Oct 2006).

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

97. United States Congress, House, Committee on Appropriations, *Department of Defense Appropriations for Fiscal Year 1983: Part 1*, Hearings, 97th Congress, 2d Session, Washington, DC: Government Printing Office, 1982.

98. United States Congress, House, Subcommittee on Cybersecurity, Science, and Research & Development. *Cybersecurity for the Homeland: Report of the Activities and Findings.* Washington, DC: Government Printing Office, 2004.

99. United States Department of Homeland Security. *Cyber Storm Exercise Report.* Washington, DC: Government Printing Office, 12 September 2006.

100. US Department of Defense. *2006 Quadrennial Defense Review*. Washington, DC: Office of the Secretary of Defense, 6 February 2006.

101. 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.

102. US Department of Defense. *Joint Vision 2020* (JV 2020). Washington, DC: Chairman of the Joint Chiefs of Staff, June 2000.

103. US Department of Defense. *Military Transformation: A Strategic Approach*. Washington, DC: Director, Force Transformation, Office of the Secretary of Defense, Fall 2003. http://www.oft.osd.mil.

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

105. US Department of Defense. *National Military Strategy for Operations in Cyberspace.* Washington, DC: Chairman of the Joint Chiefs of Staff, 2006.

106. US General Accounting Office. *Information Security - Computer Attacks at Department of Defense Pose Increasing Risks*. Washington, DC: Government Printing Office, 1996.

107. US General Accounting Office. *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO Report 04-321. Washington, DC: Government Printing Office, May 2004.

108. US Government Accountability Office. *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*. Washington, DC: Government Printing Office, September 13, 2006.

109. *USA PATRIOT ACT*, 107th CONGRESS, 1st Session H. R. 3162, October 24, 2001.

110. Verton, D. *Black Ice: The Invisible Threat of Cyber-Terrorism*. New York, NY: McGraw-Hill Osborne Media, 2003.

111. Vlahos, Michael. "The War after Byte City," in *Information Revolution and National Security*, ed. Stuart J. D. Schwartzstein. Washington, DC: The Center for Strategic and International Studies, 1996.

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

113. Wong, Kelvin. "Implementing Security: Introduction to Hacking Methods and Ways of Counter-Measure." *Swinburne Review* (Winter 2005): [23-44].

114. Wynne, Michael W. 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.