

USAF Cyberspace Command

To Fly and Fight in Cyberspace

William T. Lord, Major General, USAF

Safeguarding our own cyber capabilities while engaging and disrupting our opponents' capabilities is becoming the core of modern warfare.

—Michael W. Wynne

WE ARE a nation at war. Our military is engaged in a fight against groups and individuals who follow an ideology that has as its fundamental tenets a hostility toward our people, our beliefs, and our values. Airmen, Soldiers, Sailors, Marines, and representatives from across our government who are engaged in this bitter fight will emerge with perspectives shaped by their experiences in combat against extremists who use terror as their primary weapon to achieve their objectives. And we are also at war in cyberspace—a relatively new domain that, like air and space, crosses military, civilian, economic, and especially information aspects of our national interests.

We have already witnessed and experienced hostile incursions in cyberspace. Nothing demonstrates the contested nature of cyberspace more than how its capabilities were used to support physical attacks on our governmental and financial infrastructures on 9/11. Encrypted communications and cellular phones were used for the first attacks on the World Trade Center buildings in 1993. Aided by computer-based flight simulators, hijackers trained, planned, and funded a more successful attack. The attacks against the World Trade Center in New York had, as a secondary objective, the catastrophic degradation of the financial information upon which a large segment of the United States' economy depends.¹ Until 9/11, nonstate

Maj Gen William T. Lord is commander, Air Force Cyberspace Command (Provisional), Barksdale AFB, Louisiana. He is responsible for establishing cyberspace as a domain in and through which the Air Force flies and fights to deliver sovereign options for defense of the United States. In his current duty, he is creating the Air Force major air command for organizing, training, and equipping combat forces to operate in cyberspace. General Lord has commanded at the detachment, squadron, group, wing, and joint levels. Prior to his current position, he was director, Cyberspace Transformation and Strategy, Secretary of the Air Force Office of Warfighting Integration, and Chief Information Officer, the Pentagon, Washington, DC.

actors such as al-Qaeda were not considered threats to our national survival. But the reach, concealment, financing, and flexibility they acquired in cyberspace have allowed them to plan and execute attacks against our homeland that were considered nearly impossible just a few years ago.

In 2007, Estonia experienced a cyber attack that targeted government, media, and economic systems. The attack was insidious, rapid, and difficult to trace, and it denied service to information users for three weeks.² Much as the 2007 Chinese antisatellite missile test did for space, the incident in Estonia signaled a change in the international security environment for cyberspace. Cyber infiltrators routinely attempt to penetrate Department of Defense, government, economic, and industrial networks to gain access to information that could be vital for activities in each of these arenas. The advantages that such adversaries gain through cyberspace afford them the ability to pose serious, if not fatal, threats to our homeland. Until recently, however, our understanding of this new domain, our organization for operating in this domain, and our ability to act—offensively and defensively—was limited largely to local network operations.

The publication of the classified *National Military Strategy for Cyberspace Operations* in 2006 and the announcement by the secretary of the Air Force incorporating cyberspace into the US Air Force mission set the stage for organizing, training, and equipping forces for operations in cyberspace. Earlier this year, the Air Force chief of staff, Gen T. Michael Moseley, signed orders establishing Air Force Cyber Command (Provisional) (AFCYBER [P]). Through this new command, the Air Force will continue the process of understanding the domain and integrating capabilities required to “fly and fight” there with those that exist in the air and space domains.

The United States maintains a preeminence in warfare rarely seen in human history. Our military is adapted to defeating opposing forces in traditional combat environments, which have expanded from the land and sea battlefields to include air and space. In the emerging security environment, however, the organizations, skills, and equipment that we have used to great effect may not be enough. As scholars at the Johns Hopkins University Applied Physics Laboratory have noted, “The United States is presently encountering a national security threat different than the conventional warfare for which we have been preeminent in the world. This new threat is becoming known as ‘Unrestricted Warfare.’ . . . What is new and different is that the few can impact the many, with a

global reach enabled by advanced information technology. The first rule of unrestricted warfare is that there are no rules; nothing is forbidden.”³ In an era of unrestricted warfare, the only way to ensure that our pre-eminence in air and space remains secure is to defend our cyberspace capabilities and to hold those of our foes at risk by living and fighting virtually in the domain. This will lead us to what today are considered unconventional, distributed organizational structures but may later become standard ones as we secure and defend our cyberspace capabilities, our critical command and control (C2) nets, and hold those of our foes at risk to maintain our dominance in air and space.

These are complex tasks. Unlike traditional military systems, cyberspace capabilities are relatively cheap and easy to obtain for our adversaries and competitors, and unlike in air and space, today we have true peer competitors. To meet the challenges that cyberspace presents, the US Air Force has approached the problem carefully, examined the issues that cyberspace presents, and taken steps to address them. While the Air Force has clear responsibilities for organizing, training, and equipping its forces to operate in cyberspace as a result of its mission, this does not preclude other government agencies or military services from engaging as well—we look forward to partnering with those who do so to the mutual benefit and defense of our nation. Nevertheless, the threats in cyberspace are as vast as networks themselves and will keep coming regardless of which governmental department has the charge to defeat them.

Cyberspace A Contested Domain

The Air Force recognized that dominance in cyberspace is contested by peer competitors and, therefore, developing capabilities to operate in cyberspace must account for not only the capabilities the domain offers but also the threats it can present. Dr. Lani Kass, former director of the chief of staff of the Air Force’s Cyber Task Force, states the United States is perhaps fifth in the world in the cyber domain.⁴ An accounting of different nations’ cyberspace capabilities in table 1 confirms the scope of the competition we face in this domain.

Thus, we acknowledge that we are competitive in the cyber domain, but we are not yet dominant. The threats stem from a confluence of the very communications and computing technologies upon which our C2 networks

Table 1. 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					X

Adapted from Charles Billo 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.

depend. There is a tension between those who develop and operate systems to gain benefits from cyberspace capabilities and those who seek to exploit them. Well-documented successful attacks on the Naval War College demonstrate the need to secure our systems and to prevent the theft of our intellectual property and secrets necessary to defend our nation.⁵ Our military networks are under a constant barrage of probes and intrusions daily from threats ranging from the curious “script kiddies” to criminals seeking data to exploit about our members to nation-states seeking our secrets. Our partners in industry have also suffered losses of information. Financial and banking institutions in the US also labor under the weight of attacks of increasing sophistication as shown in figure 1.

To compete effectively in cyberspace, Airmen are already oriented toward and have been performing missions in the domain for some time. Some basic tenets of our culture lend themselves well to this work. First, the Airmen’s perspective equips us well to operate across domains—we approach national security issues and military challenges from a global perspective. This was apparent from the earliest days of our experience with airpower. Airmen were able to transit large distances with relative impunity to achieve effects against enemy surface forces, the sources of enemy industrial strength, and the enemy governments. This global perspective expanded with the addition of space capabilities and has now

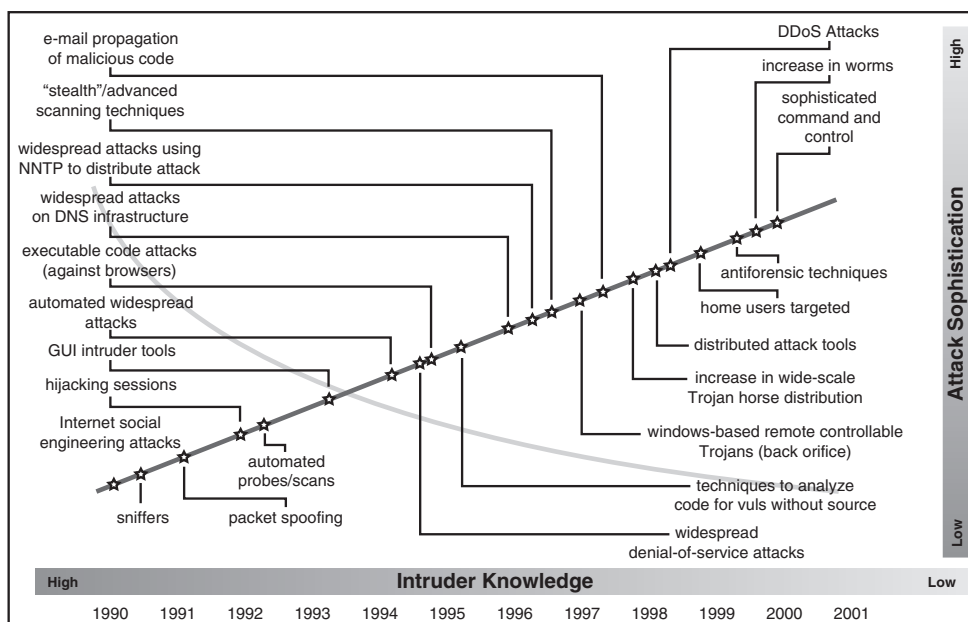


Figure 1. Cyber attack trends. (Reprinted from Carnegie Mellon CERT Coordination Center, "Incident and Vulnerability Trends, 2003," 18.)

expanded further with the multiple dimensions represented in cyberspace. This perspective does not mean that we have all the answers—it does mean, however, that our experience with the similar domains of air and space equips us well to operate in another unconstrained environment.

Our perspective was inseparable from the pace of advances in aviation and space technologies. From the aviation arms race during the First World War—in which combatants achieved innovations that translated directly into tactical and operational advantages—to the industrial production that resulted in the massive air force that fought a global war in World War II to the technological revolution that produced our space capabilities to the revolution in military affairs represented by stealth, precision targeting, and C2, Airmen forged a culture of innovation and experimentation that prepared us well for the technological challenges that operations in cyberspace present.

A global perspective combined with our technological acumen leads us to approach challenges with an eye toward achieving specific and relevant effects in air, space, and cyberspace. The earliest effects-based campaign, the Combined Bomber Offensive during World War II, aimed to dislocate what air planners characterized as the “industrial web” that sustained Axis war-making capabilities. This thought process that seeks to link tactical

actions to operational and strategic effects—some of which may be realized far from the first-order effect of the tactical mission—is part and parcel of the Airman’s culture. From our origins as a separate service—uniquely positioned to achieve strategic effects against an adversary’s war-making capabilities—we have offered our operational and national leaders sovereign options to achieve the effects they desire.

Airmen also think about effects in cyberspace as primary goals of campaigns rather than as interesting supporting capabilities for tactical missions. This does not mean that Airmen do not support joint operations or that Airmen want to conduct independent campaigns. Rather, it means that the linkages between tactical, operational, and strategic objectives drive how we think about preparing for and fighting wars. The characterization of cyberspace as a domain rather than as a tool reflects this approach. Because we treat cyberspace capabilities as primary weapons, we are particularly adept at weighing their effects on the long-term prospects of campaign success.

The above characteristics shape how the US Air Force approaches the challenge of operating in the cyber domain. Our global perspective, technological acumen, effects-based approach, and emphasis on operations in the domain as primary options for achieving national goals will shape how we build toward access, influence, and control in cyberspace and across the other domains in the future. The establishment of a new major command is the first step on this journey toward integrating capabilities across air, space, and cyberspace.

A New Kind of Major Command Both Virtual and Distributed

Secretary of the Air Force Michael Wynne was certainly aware that adding cyberspace to the Air Force mission would not be enough either to secure our interests or to develop credible operational capabilities in the domain. There must be a cyberspace advocate within the Air Force to fulfill the Title 10 “organize, train, and equip” responsibilities—in other words to provide an organization charged with harmonizing cyberspace capabilities with those in air and space, to train specialized warriors, and to procure and field relevant systems for operating in that domain. This advocacy is essential—the people, organizations, and missions in the Air Force’s cyberspace enterprise require high-level support if they are to succeed.

In creating the command, Secretary Wynne foresaw the opportunity to lead the Air Force into the twenty-first century. He challenged AFCYBER (P) leaders to “lead turn the AF into the future, building the first 21st century command.” It needed to be unlike the typical “brick and mortar industrial age command.” It needed to be virtual. Guided by this vision, members of AFCYBER (P) are working diligently to build an organization as agile as the domain within which it operates. When it achieves initial operating capability on or about 1 October 2008 as a major command on par with the other major commands, AFCYBER (P) will ensure the Air Force delivers the required war-fighting capabilities to the combatant commanders while also defending our operational infrastructure. For now, the provisional command’s mission is to ensure the rapid establishment of this new command by publishing a program plan to organize it, preparing program objective memorandum submittals and a budget baseline, and developing criteria for basing new portions of the command.

AFCYBER (P) Mission and the National Ends, Ways, and Means

Sovereign options refer to the spectrum of choices air, space, and cyberspace capabilities offer US policy makers for solving problems.

—Michael W. Wynne

Various arms of the US government exist to develop options across the spectrum of its diplomatic, informational, military, economic, and cultural (DIME-C) means to meet the national ends. The Air Force exists to serve national policies, and the Air Force Cyberspace Command will ensure that the Air Force can do its part in supporting the national strategy to secure cyberspace.⁶ As discussed above, there are unique characteristics of Air Force culture that make the Air Force particularly suited to operating in cyberspace. However, the Air Force’s focus is on preserving its ability to access and maneuver within cyberspace and in the air and space domains while preventing our adversaries from doing the same. This leads the Air Force to focus on developing capabilities that lead toward cross-domain access, influence, and control while better integrating kinetic and nonkinetic effects. The true power of cyber lies in the creation of synergy by integrating with air and space.

The AFCYBER (P) mission and vision statements define who we are, why we exist, and what we seek to achieve. Specifically,

Our mission is to provide combat ready forces trained and equipped to conduct sustained combat operations through the electromagnetic spectrum and fully integrate these operations with air and space operations.⁷

Our vision statement defines our nonnegotiable commitment to deliver USAF sovereign options for the United States through cross-domain dominance of air, space, and cyberspace.

Secure our nation by employing world-class cyber capabilities to dominate the cyberspace domain, create integrated global effects, and deliver sovereign options.⁸

Make no mistake: if we cannot dominate in cyberspace, we place air and space dominance at risk. For example, if an adversary is able to inject malicious software into the F-22 fleet, we may not be able to fly the Raptor when it is needed in battle. Similarly, if an adversary jams or dazzles the GPS constellation, precision strike may not be possible. The Air Force can neither afford unnecessary collateral damage caused by negation of our cyber capabilities nor can we achieve victory on the battlefield without cyber dominance.

As mentioned earlier, the Air Force has chosen to move forward in cyberspace by establishing a new major command. By leveraging a modern, robust, unified communications architecture (i.e., merging of telephone and data networks), AFCYBER (P) will be able to create a virtual command from distributed centers of excellence. At first blush, cynics may claim that going virtual is a solution looking for a problem. However, the facts do not support that conclusion. The virtual command construct paves the way for optimizing partnerships across the Air Force major functional areas. Using a model pioneered by corporate counterparts, AFCYBER (P) will place a headquarters presence with or near strategic partners to facilitate stronger alliances. For example, placing key staff near research centers, logistics supply points, and combatant commands facilitates and thus establishes and maintains strong, face-to-face ties with partners in those functions. So far, AFCYBER (P) has identified 11 such locations where partnerships are vital for mission success. This organizational model shifts the emphasis from organizing to support communications within the command to supporting communications and relationships with other commands and partners. These partnerships come in many forms, including participation in the National Counterintelligence Joint Task Force, which includes participation

from the FBI and much of the national intelligence community. It also involves day-to-day coordination between the Defense Cyber Crime Center (for which the Air Force is executive agent) and all other departments of the federal government. Numerous discussions with our NATO allies and partners have been ongoing since the inception of this provisional command. These broad relationships give us access to capabilities well beyond those the Air Force currently possesses and greatly improves our means to achieve national ends. This includes leveraging the Air Force's significant investment in National Guard and Reserve forces.

The National Guard and Reserve are already fundamental to the functioning of the Air Force's cyberspace capabilities. The majority of force structure the Air Force has today in providing expeditionary, or combat, communications resides in the Air Guard and AF Reserve, and the new command will inherit responsibility for all of it. Likewise, over 90 percent of Air Force personnel capable of engineering and installing large communications systems exist only in the Guard and Reserve. Aside from communications-related activities, unique, cyberspace-focused units have already been created and contribute to the total force. The 262nd Information Warfare Aggressor Squadron, a Guard unit out of Seattle, Washington, is one of the first Guard units created to address new cyberspace missions, but there will be many more. Total Force elements will be at the core of the Air Force's Cyberspace Command's operations, spanning every level of the cyberspace enterprise from unit level all the way to command headquarters and the air operations center.

Not only will the virtual headquarters leverage long-standing relationships with the Total Force and other functionals and agencies, it will also provide the command with much greater means to effect operations across the spectrum of conflict. The Air Force already has an extensive collection of capabilities that will fall under control of the new command but will not physically relocate. For example, the distributed nature of the command allows us access to established and operating networks and their operators along with fully functioning physical plants. Bringing these mission sets under the authority of one operational commander opens doors for better synchronization of resources.

Another issue critical to fulfilling Air Force Title 10 responsibilities involves establishing and developing a specialized career force through the creation of a new Air Force specialty code (AFSC) series for enlisted and officer forces. The new cyberspace career field will include a diverse mix of

skills to cover the span of mission areas that range from information operations to electronic warfare, communications and intelligence, expeditionary cyber capabilities, and network warfare. Many years of expertise exist in cyberspace-related functions today. We will harness this intellectual capital and focus on developing a new form of orientation known as “cyber-mindedness.”⁹ Similar to the concept of “air-mindedness” already imbued into every Airman, cyber-mindedness involves the unhindered development of cyberspace capabilities to achieve desired effects.

Air Force Cyberspace Command will consist of a headquarters, one numbered air force, and four wings organized as depicted in figure 2. While many of cyberspace’s capabilities cost little in terms of actual hardware, this is not to say that no additional resources are required to realize dominance in cyberspace. On the contrary, some cyberspace capabilities will require integration into traditional military missiles and aircraft with all the attendant costs. Supplemental training for the new cyberspace career field will also be required. Certainly network-specific programs to defend and integrate Air Force effects across air, space, and cyberspace will be critical to the future improvement of the effectiveness of our cyberspace forces. Although underpinned by technology, mission considerations drive AFCYBER’s path to virtualization. Matching the command’s organizational structure and operating philosophy to the domain within which it will function provided the Air Force strategic agility while retaining the ability to meet emerging challenges.

Challenges on the Road to Dominance in Cyberspace

Although we do not anticipate requesting changes in law to accommodate cyberspace operations yet, we will lean heavily on existing statutes to work through some particularly thorny legal challenges required in the cyber domain. Some of these legal challenges include the boundaries between law enforcement, intelligence, and military activities. For example, while AFCYBER can execute certain tasks such as defending critical military infrastructure inside the CONUS based on Title 10 responsibilities—and we will present AFCYBER forces to the COCOMS to carry out that mission—if the attackers are criminals, our partners in the FBI and other agencies must counter these activities by exercising Title 18 law enforcement authorities. The Title 50 authorities vested in the intelligence community are also essential to efficient and legal operations within cyberspace.

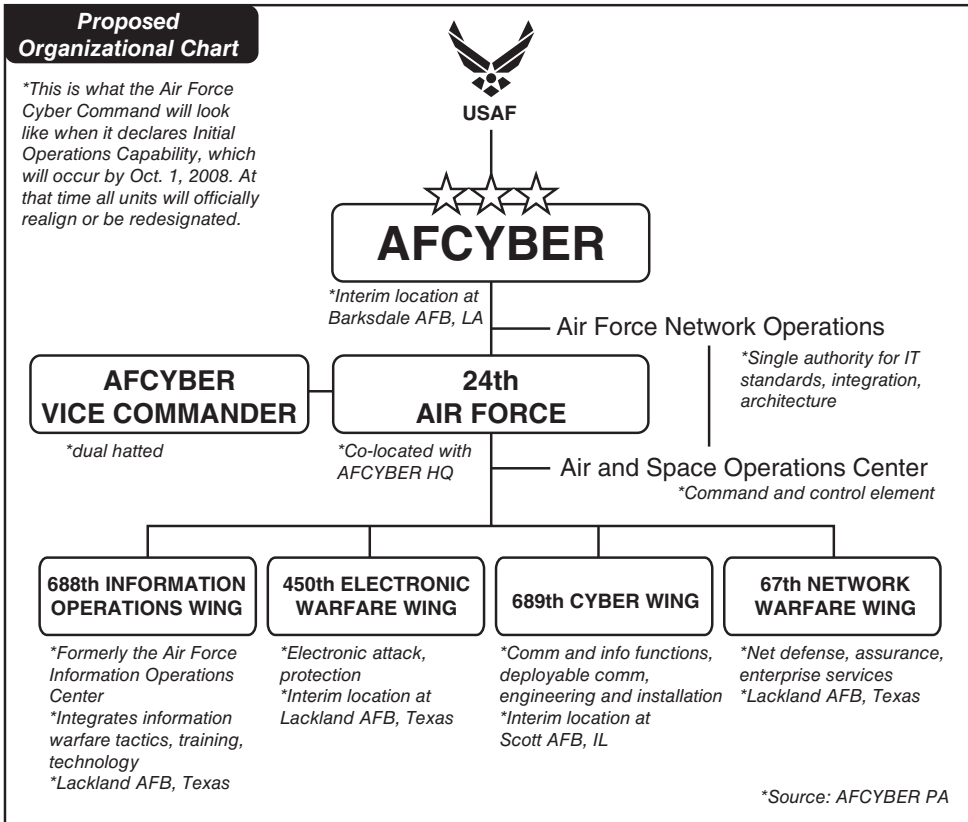


Figure 2. Proposed organizational chart


Operational challenges overshadow the legal challenges, and most center around the pace at which cyberspace threats present themselves compared to our present speed in responding. Globalization has created an unprecedented interdependency between the national economies that can cause a very rapid shift from peace to conflict. Ensuring that sufficient authorities to blunt a cyberspace attack are in place and understood is critical to guarantee that our government and our Air Force can respond in time.

The opening salvo of a cyberspace-based attack could potentially leave our air and space capabilities in disarray, thus leveling the playing field for our adversaries in other domains. This is why the Air Force seeks the capability to defend its cyberspace, and especially its C2 and weapons systems, from cyber attacks and to dominate our foes in this domain. The Air Force is not seeking to usurp the authorities of anyone; rather, it seeks to develop

specific cyberspace intelligence and weaponry to create effects that preserve its ability as an air force to fight in air, space, and cyberspace. Keeping up with the rapid pace of development in cyberspace capabilities will be one of the most difficult tasks the command faces. In an austere budget environment, keeping up with new technologies and the threats they present can be an expensive and consuming task. Funds to refresh technology and weapons and to maintain excellent analytical capabilities will be required.

The most expensive and difficult task will be recruiting and retaining a workforce necessary to achieve dominance in this arena. Because these skills are so marketable in commercial industry, access to talent will become a critical factor in cyberspace war fighting. I say access to talent because we will require unconventional approaches to obtain talent we could not otherwise afford. Access to part-time patriotic experts over AFCYBER's virtual enterprise may be crucial to success in this area. This will require a cultural shift within the Air Force to allow us to leverage the skills that we would otherwise be unable to develop through our traditional force development programs.

Concluding Thoughts

We are often reminded that we live in uncertain times and that uncertainty comes from the many emerging disruptive threats. Cyberspace presents both potential threats but also promises to advance our war-fighting capabilities substantially. AFCYBER (P) has begun to move the ball forward by integrating with air and space in ways our fathers could never have imagined. We are on track to deliver on the commitment to create an operational cyberspace command by 1 October 2008, which will provide a coherent initial operating capability to defend the Air Force's capabilities across all domains while respecting the authorities of other departments and agencies. With strong investments in training our cyberspace warriors and developing the tools they require, the command will preserve the heritage and traditional role of the Air Force as America's first choice for achieving strategic, operational, and tactical effects. Most importantly, AFCYBER (P) will integrate with air and space to provide the global reach, power, and vigilance to preserve our nation's security for the future. For the good of the nation, we must meet the challenges that cyberspace presents to preserve our ability to achieve our national goals and to provide security for ourselves, our partners, and our allies. 

Notes

1. On the effects of the 9/11 attacks against the World Trade Center, Osama bin Laden said, "And if the fall of the twin towers was a huge event, then consider the events that followed it. . . . Let us talk about the economic effects that are still continuing. According to their own admission, the share of the losses on the Wall Street Market reached 16 percent." See Bruce Lawrence, ed., *Messages to the World: The Statements of Osama bin Laden* (New York: Verso, 2005), 111.
2. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, 17 May 2007, <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.
3. Johns Hopkins University Applied Physics Laboratory, "What is Unrestricted Warfare?" http://www.jhuapl.edu/urw_symposium/previous/2007/index.htm.
4. Dr. Lani Kass, former director of the CSAF Cyberspace Task Force, has commented widely that the United States is "fifth" in the world in attaining dominance in cyberspace.
5. Bill Gertz, "Chinese Hackers Prompt Navy College Site Closure," *Washington Times.com*, 30 November 2006, <http://www.washingtontimes.com/national/20061130-103049-5042r.htm>.
6. *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), ix, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.
7. US Air Force Fact Sheet, AFCYBER (P) Vision Statement, <http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10786>
8. Ibid.
9. Lt Col Sebastian M. Convertino II, CDR Lou Anne DeMattei, and Lt Col Tammy Knierim, *Flying and Fighting in Cyberspace*, Maxwell Paper no. 40 (Maxwell AFB, AL: Air University Press, July 2007), 69.