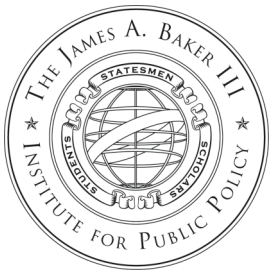

James A. Baker III Institute for Public Policy
Rice University

Off We Go ...
Cyberspace, the Air Force and the New Face of Battle

BY

Christopher Bronk, Ph.D.
Fellow in Technology, Society and Public Policy
James A. Baker III Institute for Public Policy
Rice University

August 8, 2008

The following opinion piece was written by a researcher, fellow or scholar. The research and views expressed in this opinion piece are those of the individual(s), and do not necessarily represent the views of the James A. Baker III Institute for Public Policy.

On Nov. 2, 2006, then-Secretary of the Air Force Michael Wynne laid the foundation for his service's move to develop its status as the leader in network warfare operations at the U.S. Department of Defense by announcing the formation of a new element of the United States Air Force (USAF) intended to conduct military operations in cyberspace. With the Air Force providing the significant contributions to the War on Terror in aerial surveillance, largely conducted by unmanned aircraft and the unglamorous but vitally necessary airlift mission, the traditional areas of endeavor for the 61-year-old service — strategic bombing and fighter missions — have diminished in importance. Whereas the Air Force bought hundreds of F-15 Eagles to deter the Soviets during the tail end of the Cold War, it is now only authorized to buy fewer than 200 F-22 Raptors to replace them. This metric alone indicates just how radically the Air Force is changing.

Finding new missions for the service is important in the struggle for part of a Pentagon budgetary pie that is likely to shrink with the arrival of a new administration in January. As a maneuver of inside-the-Beltway bureaucratic process, the move into cyberspace is pragmatic and shrewd, but politics threaten to impede the construction of a military organization capable of meeting its mandate. The specter of cyber-security, the protection of computer networks from malicious actors, has been on the Pentagon agenda for more than a decade. Be they loosely confederated electronic joyriders or the intelligence services of major world powers, those who penetrate or disrupt computer networks pose a real threat to national security — it's just difficult to assess how large a threat they represent. Certainly the cyber-attacks launched against Estonia in 2007 — after the government there upset Moscow by moving a memorial to the Great Patriotic War from downtown Tallinn to a suburb — elevated the cyber-security issue in the national security mindset.

Translating cyber-security from a vague but growing threat and a funding opportunity into doctrine and real operational capability has largely been handled by the Air Force. This process is now at a pivotal point. Last month, the assistant secretary for installations, environment and logistics solicited input from 18 state governors in selecting the optimal location for Cyber Command's headquarters, which is envisaged to stand as a major functional component of the USAF. Seeking to enlist the maximum level of support across congressional districts around the

country, Cyber Command's leadership assembled a large organization in less than two years, tapping active and reserve units around the United States and overseas to be organized under four wings. Three of them are based at Lackland Air Force Base, with another unit slated for Brooks Air Force Base. With so much of Cyber Command's mass concentrated near San Antonio, it makes a good deal of sense for its headquarters to reside there too.

While we will have to wait until September 2009 for the announcement of Cyber Command headquarters' permanent home, some issues should be considered in the interim. Top among them is the role of the other services, which are developing cyber capabilities of their own, in working jointly on the strategy, tactics and resources required to engage in cyber conflict. Strong linkages to one of the jointly staffed higher headquarters, possibly Strategic Command, should be considered to avoid counterproductive interservice squabbles and wasteful duplication of resources. In addition, Cyber Command will require clear and ethical rules and regulations regarding the use of its tools. The often-venomous debate on Capitol Hill regarding wiretapping offers a lesson in how not to develop capabilities considered controversial by many in the Information Technology industry. Finally, there is the matter of how Cyber Command will relate to America's allies around the globe. A recent rewrite of U.S. Navy strategy urged the need to cooperate with foreign partners in keeping the world's oceans, which serve as the transit route for an overwhelming majority of global trade, secure. This is a good template for national cyber-security policy. What we need to avoid is a rhetoric in which we are constantly at war in cyberspace and in which we stand alone in our efforts, exerting our dominance. Cyber Command will ultimately fail without the aid and support of the large community of nations eager to make use of the Internet for the greatest universal social and economic gain.