GlobalResearch
Center for Research on Globalization

Air Force Pulls the Plug on Cyber Command

By Tom Burghardt

Theme: US NATO War Agenda

Global Research, August 18, 2008
Antifascist Calling... 18 August 2008

In July, ***Antifascist Calling*** reported on the imminent launch of U.S. Air Force Cyber Command (**AFCYBER**).

With a unified organizational structure and a $2 billion budget for its first year of operations, and a projected $30 billion cost for the first five years of operations, AFCYBER promised an offensive capability that would deliver withering attacks on adversaries.

As I wrote, "Eventually, if Air Force securocrats have their way, it 'will grow into one of the service's largest commands.' With a mission to 'deceive, deny, disrupt, degrade, and destroy' an enemy's information infrastructure, the potential for mischief on the part of American 'warfighters' and 'public diplomacy' black propaganda specialists shouldn't be underestimated."

Now however, numerous reports reveal that the Air Force has suspended plans for the controversial unit. ***NextGov*** broke the story Wednesday. According to investigative journalist Bob Brewin,

> The Air Force on Monday suspended all efforts related to development of a program to become the dominant service in cyberspace, according to knowledgeable sources. Top Air Force officials put a halt to all activities related to the establishment of the Cyber Command, a provisional unit that is currently part of the 8th Air Force at Barksdale Air Force Base in Louisiana, sources told NextGov.
>
> An internal Air Force e-mail obtained by NextGov said, "Transfers of manpower and resources, including activation and reassignment of units, shall be halted." Establishment of the Cyber Command will be delayed until new senior Air Force leaders, including Chief of Staff Norton Schwartz, sworn in today, have time to make a final decision on the scope and mission of the command. ("Air Force Suspends Cyber Command Program," NextGov, August 13, 2008)

Air Force spokesman Ed Gulick told ***Federal Times***, the "freeze" was necessary "because we have new leaders and they want to make sure they're on the right course." But he said the Air Force "remains committed to cyberspace."

With an October 1 launch date, it appears that aggressive efforts by Major General William Lord, the unit's commander, to hype its capabilities may have been its undoing. Brewin reports the "hard sell" by Lord and other AF securocrats "seemed to be a grab by the Air Force to take the lead role" in U.S. cyberdefense efforts.

Bureaucratic in-fighting may play a significant role in pulling AFCYBER's plug. Philip Coyle, a

senior adviser with the Center for Defense Information (**CDI**), a liberal defense think tank, told *NextGov* that he believes "the Navy's Network Warfare Command and the Space and Naval Warfare Systems Center have led the way in cyberspace. The Army engages in cyberspace operations daily in Afghanistan and Iraq, said Coyle, who served as assistant secretary of Defense and director of its operational test and evaluation office from 1994 to 2001."

Accordingly, Coyle believes the decision may have come from Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, who wants to see a more "robust role" for the Navy in cyberspace. Lord's high public profile and hard-sell may have shot-down AF plans to "dominate cyberspace" and the AF "is now suffering from its own hubris."

It appears that AFCYBER's aggressive public posture and its assertion that cyberspace is a "warfighting domain," may have angered Department of Defense bureaucrats who favor a "softer" approach when it comes to plans for imperialist domination.

In this light, recent Air Force scandals, including the unauthorized transfer of nuclear weapons in 2007 and the dismantling of the service's top command by Secretary of Defense Robert Gates as a result, the Air Force's lax organizational structure may have been a deciding factor.

In June, Gates fired Air Force Chief of Staff Gen. Michael Mosley and Air Force Secretary Michael Wynne for their incompetence over the service's handling of nuclear weapons.

Many readers will recall that on August 30, 2007 a B-52 Stratofortress bomber flew nearly 1,500 miles from Minot Air Force base in North Dakota to Barksdale Air Force Base in Louisiana with six nuclear-tipped cruise missiles fixed to its wings. For nearly six hours the Air Force was unable to account for the weapons. When *Military Times* broke the story, it elicited a yawn from major media outlets that amounted to self-censorship.

While brief media reports emphasized that the public was "never in danger," as physicist Pavel Podvig **reported**,

> The point is that the nuclear warheads were allowed to leave Minot and that it was surprised airmen at Barksdale who discovered them, not an accounting system that's supposed to track the warheads' every movement (maybe even in real time). We simply don't know how long it would've taken to discover the warheads had they actually left the air force's custody and been diverted into the proverbial "wrong hands." Of course, it could be argued that the probability of this kind of diversion is very low, but anyone who knows anything about how the United States handles its nuclear weapons has said that the probability of what happened at Minot was also essentially zero. ("U.S. loose nukes," Bulletin of the Atomic Scientists, 12 September 2007)

In the wake of the scandal, Mosley and Wynne were forced to fall on their swords. Similar forces may be at play regarding AFCYBER. According to **CDI** researcher Chelsea Dilley,

> It is unclear what AFCYBER's exact mission is, what capabilities are being developed, what circumstances warrant a cyber attack, what actions will be taken in response to an attack, who can authorize an attack, what steps will be taken to prevent crisis escalation, what the budgets are and exactly where the

> money is coming from. AFCYBER's relation to the Department of Homeland Security and to the Air Force Space Command is also hazy, which could prove problematic, as all have claimed some responsibility for maintaining control of cyberspace.
>
> Alarmingly, there are many similarities in the ways used to promote AFCYBER and those used in the Air Force's increasingly belligerent counterspace mission. The diction used in the 2004 Air Force Counterspace Operations Doctrine and the 2008 Air Force Cyber Command Strategic Vision is in many places exactly the same, and it is uncertain if the task that was given to the Air Force Space Command to maintain cyberspace has actually been transferred to or just appropriated by the new Cyber Command. ("Air Force Cyber Command: Defending Cyberspace, or Controlling It?," Center for Defense Information, August 7, 2008)

Whether or not a bureaucratic tussle amongst competing branches of the military and the Department of Homeland Security may have played a role in AFCYBER's apparent demise, the Air Force is continuing to develop new and more hideous weapons to insure that the American Empire's dream of global domination remains a viable option for our capitalist masters.

New Scientist **reported** August 12 on an airborne laser weapon, dubbed the "long-range blowtorch." According to defense analyst David Hambling,

> The Advanced Tactical Laser (ATL) is to be mounted on a Hercules military transport plane. Boeing announced the first test firing of the laser, from a plane on the ground, earlier this summer.
>
> Cynthia Kaiser, chief engineer of the US Air Force Research Laboratory's Directed Energy Directorate, used the phrase "plausible deniability" to describe the weapon's benefits in a briefing on laser weapons to the New Mexico Optics Industry Association in June. ("U.S. Boasts of Laser Weapon's 'Plausible Deniability'," New Scientist, August 12, 2008)
>
> As readers are aware, "plausible deniability" is a term used to describe aggressive covert operations where those responsible for an event, say the assassination of a political opponent or the terrorist bombing of a civilian target, could plausibly claim to have neither knowledge nor involvement in the atrocity since command responsibility by design is highly compartmentalized.

According to Hambling, "a laser is silent and invisible. An ATL can deliver the heat of a blowtorch with a range of 20 kilometres, depending on conditions. That range is great enough that the aircraft carrying it might not be seen, especially at night."

Whatever the eventual fate of AFCYBER rest assured, as *Aviation Week* **reported** back in December, "U.S. Air Force leaders working on the nascent cyber command believe there will be a 'huge' need for contracted services to support the embryonic effort as it faces personnel, technology and funding headwinds."

Army, Navy, Air Force? Who cares! Enterprising corporate grifters will certainly be there, pushing for "full-spectrum dominance" as they lunge after multiyear, high-end contracts that just might hit the corporatist "sweet spot"!

Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition

*to publishing in Covert Action Quarterly, Love & Rage and Antifa Forum, he is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by **AK Press**.*

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/