Air Force Cyber Command: Building the Infrastructure for High-Tech War Crimes

By Tom Burghardt
Global Research, July 19, 2008
Antifascist Calling... 19 July 2008

Theme: Militarization and WMD, Police State & Civil Rights

What do you get when you combine U.S. militarism, fantasies of domination and an administration that views the internet as a hot-bed of "evil-doers" and "subversives"? Cyber Command, of course! Only this scheme has the potential of inflicting massive suffering on civilian populations across the planet.

Currently situated at the secretive Barksdale Air Force Base in Louisiana, **Air Force Cyber Command**, the newest Pentagon command since the 1990s, is dedicated to the notion that the "next war" will be fought in the electromagnetic spectrum, one that envisions computers as "network-centric" weapons.

With a unified organizational structure and a $2 billion budget for the first year of operations, Cyber Command is touted as the next "big thing." According to a recent piece in ***Air Force Times***, Cyber Command "has established 17 new enlisted and officer Air Force Specialty Codes — creating major changes in the career paths of more than 32,000 airmen."

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.

Although the "**Strategic Vision**" proffered by the Air Force is couched in defensive language, by its very nature Cyber Command represents a *qualitative* leap by the Pentagon towards creating an offensive capability, one with far-reaching and potentially catastrophic consequences for societies that fall under the baleful gaze of American cyberwarriors.

This is clearly spelled out by Air Force theorists. In their view, the "strategic environment" confronting imperialism is described as "unpredictable and increasingly dangerous," characterized "by the confluence of globalization, economic disparities, and competition for scarce resources."

And as "economic disparities" grow ever-more glaring, newer and more effective means for obtaining "compliance" are required by our corporate masters and their militarist attack dogs. This is underscored by Cyber Command's stated goal "to achieve situational dominance *at a time and place of our choosing*." [emphasis added] According to the Air Force,

> Global vigilance requires the ability to sense and signal across the

> electromagnetic spectrum. Global reach requires the ability to connect and transmit, using a wide array of communications networks to move data across the earth nearly instantaneously. Global power is the ability to hold at risk or strike any target with electromagnetic energy and ultimately deliver kinetic and non-kinetic effects across all domains. These cyberspace capabilities will allow us to secure our infrastructure, conduct military operations whenever necessary, and degrade or eliminate the military capabilities of our adversaries. (Air Force Cyber Command, "**Strategic Vision**," no date)

According to ***Wired*** defense analyst Noah Shachtman,

> The Air Force wants a suite of hacker tools, to give it "access" to — and "full control" of — any kind of computer there is. And once the info warriors are in, the Air Force wants them to keep tabs on their "adversaries' information infrastructure completely undetected." …
>
> Traditionally, the military has been extremely reluctant to talk much about offensive operations online. Instead, the focus has normally been on protecting against electronic attacks. But in the last year or so, the tone has changed — and become more bellicose. "Cyber, as a warfighting domain . . . like air, favors the offense," said Lani Kass, a special assistant to the Air Force Chief of Staff who previously headed up the service's Cyberspace Task Force. ("Air Force Aims for 'Full Control' of 'Any and All' Computers," Wired, May 13, 2008)

How might this play out in the megacities of the global south, identified by Pentagon planners as "the strategic high ground" of the 21st century?

Durham University geographer Stephen Graham **describes** the ideological mind-set guiding contemporary Pentagon doctrine thusly: On a theoretical level military strategists, particularly proponents of "network-centric warfare"–the Rumsfeldian "Revolution in Military Affairs" (RMA)–believe that dominance can be achieved through "their increasingly omnipotent surveillance and 'situational awareness', devastating and precisely-targeted aerial firepower, and the suppression and degradation of the communications and fighting ability of any opposing forces."

An integrated process in other words, that draws from contemporary corporate management theory to create "continuous, always-on support for military operations in urban terrain." Call it the deranged "battlespace" where Wal-Mart morphs into The Terminator. Graham writes,

> The overwhelming rhetoric in such efforts emphasises that new military techno-science, specifically developed to address cities, will turn global south urban environments into areas that US forces can completely dominate, using their technological advantages, with minimum casualties to themselves. New weapons and sensor programmes, specifically designed to enhance the ability of future US forces to control and dominate global south cities through network-centric means, are already emerging from the wider efforts at physical and electronic simulation, wargaming, and the evaluation of the experience of the Iraq insurgency. These centre, first, on unveiling global south cities through new sensor technologies, and, second, on developing automated and robotic weapon systems linked to such sensors. ("From Space to Street Corner: Global South Cities and US Military Technophilia," Unpublished paper, 2007)

How might Cyber Command fit into the mix? Under the heading "Cyberspace Attack Operations," Air Force theorists aver,

> Cyberspace effects gained from emerging technology, such as directed energy, include: sensor disruption, data manipulation, decision support degradation, command and control disruption, and weapon system degradation. Cyberspace attacks can be conducted on an adversary's terrestrial, airborne, and space-based communication infrastructure as well as his forces, equipment and logistics.

Indeed such operations are fully theorized as a means of achieving "full-spectrum dominance" via "Cyberspace Offensive Counter-Operations,"

> Cyberspace favors offensive operations. These operations will deny, degrade, disrupt, destroy, or deceive an adversary. Cyberspace offensive operations ensure friendly freedom of action in cyberspace while denying that same freedom to our adversaries. We will enhance our capabilities to conduct electronic systems attack, electromagnetic systems interdiction and attack, network attack, and infrastructure attack operations. Targets include the adversary's terrestrial, airborne, and space networks, electronic attack and network attack systems, and the **adversary itself**. As an adversary becomes more dependent on cyberspace, cyberspace offensive operations have the potential to produce greater effects. ("Strategic Vision," op. cit.) [emphasis added]

"Greater effects" in this context mean nothing less than the capability of rendering "target" societies completely vulnerable to imperialist attack. Nearly a decade ago, NATO forces dropped what was described as a graphite "**blackout bomb**," the BLU-114/B "soft-bomb" on Belgrade and other cities during its aggressive war against the remnants of the former Yugoslavia–with devastating effects. Marty Mclaughlin **wrote**:

> A particularly dangerous consequence of the long-term power blackout is the damage to the water systems in many Yugoslav cities, which are dependent on pumping stations run by electrical power. Novi Sad, a city of 300,000 which is the capital of the Vojvodina province of Serbia, has been without running water for eight days, according to residents. Families have been compelled to get water from the Danube river to wash and operate the toilet, and a handful of wells to provide drinking water.
>
> Sewage treatment plants have also been shut down, with the result that raw, untreated sewage has begun to flow into the network of rivers that feed into the Danube, central Europe's most important waterway. ("Wall Street celebrates stepped-up bombing of Serbia," World Socialist Web Site, May 5, 1999)

With technological advances, imperialist cyberwarriors believe they can simply turn an adversary's networked infrastructure into a "zombie" system under its control to achieve the same, if not greater, devastation. As Marty Graham reported in ***Wired***,

> Comparisons between nuclear and cyberweapons might seem strained, but there's at least one commonality. Scholars exploring the ethics of wielding logic bombs, Trojan horses, worms and bots in wartime often find themselves

> treading on ground tilled by an earlier generation of Cold War nuclear gamesmen.
>
> "There are lots of unknowns with a cyberattack," says Neil Rowe, a professor at the Center for Information Security Research at the U.S. Naval Postgraduate School, who rejects cyberattacks as a legitimate tool of war. "The potential for collateral damage is worse than nuclear technology…. With cyber, it can spread through the civilian infrastructure and affect far more civilians." ("Welcome to Cyberwar Country, USA," Wired, February 11, 2008)

Which is precisely *why* the Air Force has expressed an interest in building a robust Cyber Command!

According to an Air Force Fact Sheet, "**Cyberspace 101**," they conceive their "mission" as one that will "afford us offensive capabilities and deliberate target sets."

With an official launch date set for October 1, 2008, Cyber Command as yet has no permanent home but one can predict that the congressional "leader" who can deliver the goods for his "constituents" will reap the rewards of a long-term basing agreement. From Hampton, Virginia to Yuba City, California, local "leaders" are falling all over themselves with sweetheart deals negotiated behind the backs of their citizens.

And according to ***Wired***, prospective local "stakeholders" are "throwing in offers of land, academic and research tie-ins, and, in one case, an $11 million building with a moat."

With billions of dollars in "outsourced" government contracts hanging in the balance, Cyber Command is no laughing matter. Back in December, *Aviation Week* **reported** that "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." Michael Bruno wrote,

> "There's going to be a huge contracting requirement," said Maj. Gen. Charles Ickes II, Air National Guard special assistant to the deputy chief of staff for operations, plans and requirements.
>
> "I don't think anyone can tell you how big," he told the Northern Virginia chapter of the Armed Forces Communications and Electronics Association's Air Force information technology conference Dec. 5. ("New Cyber Command to be 'Huge' Business Opportunity," Aviation Week, December 6, 2007)

In May, *Washington Technology* **reported** that the Air Force "is calling for white papers on how it might conduct successful offensives against cyberspace adversaries." And to back-up its call, the Air Force Research Laboratory (**AFRL**) is offering $11 million in funding for the proposed two-year project.

If past Pentagon projects are any indication of where AFRL proposals may lead, the estimated $30 billion cost for its initial 5-year project has the all the hallmarks of another massive taxpayer-funded black hole for enterprising defense contractors.

Indeed, the Defense Advanced Research Projects Agency (DARPA) will play a critical role for the Air Force and is currently designing a "National Cyber Range" that "will create a virtual environment where the Defense Department can mock real warfare, both defense and

offense," according to ***Wired*** defense analyst Sharon Weinberger.

According to an announcement posted on the Federal Business Opportunities **website**, the project, designed by DARPA's **Strategic Technology Office**, is described as a test zone that will enable the state "to conduct cyber operations by providing a persistent cyber range." Many of the program details are classified.

Envisioned as a force conducting "sustained offensive and defensive operations throughout the electromagnetic spectrum fully integrated with air and space operations," Air Force Cyber Command will "leverage...cyberspace capabilities...in all domains, to create global and theatre effects in support of the Joint warfighting team."

War crimes at the push of button? The future is *now* and its looking mighty grim.

*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/