GlobalResearch
Center for Research on Globalization

The Pentagon's Cyber Command: Formidable Infrastructure arrayed against the American People

By Tom Burghardt
Global Research, April 26, 2009
Antifascist Calling... 26 April 2009

Region: USA
Theme: Police State & Civil Rights, US NATO War Agenda

The Wall Street Journal **revealed** April 24 that current National Security Agency (NSA) director Lt. General Keith Alexander will "head the Pentagon's new Cyber Command."

Friday's report follows an April 22 **piece** published by the *Journal* announcing the proposed reorganization. The Obama administration's cybersecurity initiative will, according to reports, "reshape the military's efforts to protect its networks from attacks by hackers, especially those from countries such as China and Russia."

When he was a presidential candidate, Obama had pledged to elevate cybersecurity as a national security issue, "equating it in significance with nuclear and biological weapons," the *Journal* reported.

The new Pentagon command, according to ***The Washington Post***, "would affect U.S. Strategic Command, whose mission includes ensuring U.S. 'freedom of action' in space and cyberspace, and the National Security Agency, which shares Pentagon cybersecurity responsibilities with the Defense Information Systems Agency."

How Cyber Command's launch would effect civilian computer networks is unclear. However, situating the new agency at Ft. Meade, under the watchful eyes of National Security Agency snoops, should set alarm bells ringing.

Charged with coordinating military cybersecurity programs, including computer network defense as well as a top secret mission to launch cyber attack operations against any and all "adversaries," the new command has been mired in controversy ever since the U.S. Air Force declared it would be the lead agency overseeing Cyber Command with the **release** of its "Strategic Vision" last year.

Since that self-promotional disclosure however, multiple scandals have rocked the Air Force. In 2007, a B-52 Stratofortress bomber flew some 1,500 miles from Minot Air Force Base in North Dakota to Barksdale Air Force Base in Louisiana with six *live* nuclear-tipped cruise missiles affixed to its wings. For nearly six hours, the Air Force was unable to account for the missing weapons. While the scandal elicited scarcely a yawn from the corporate media, physicist Pavel Podvig **wrote**,

> 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)

As a result of the affair and numerous **procurement scandals**, Air Force Chief of Staff Gen. Michael Mosley and Air Force Secretary Michael Wynne were fired by Secretary of Defense Robert Gates for incompetence. Numerous defense analysts believe this was a major reason why the Air Force was supplanted as the lead Cyber agency.

While one can reasonably support government efforts to protect critical infrastructure such as electrical grids, chemical plants, nuclear power stations or the nation’s air traffic control system from potentially devastating attacks that would endanger the health and safety of millions of Americans, these goals can be achieved by writing better programs. Yet from its inception, Cyber Command has been theorized as a nodal point for launching crippling attacks against the civilian and military infrastructure of imperialism’s enemies.

As I **reported** last July, Air Force Cyber Command (AFCYBER) is centered at the secretive Barksdale Air Force Base. At the time, AFCYBER had a unified command structure and a $2 billion budget through the first year of its operations.

The *Air Force Times* **reported** last year that AFCYBER “has established 17 new enlisted and officer Air Force Specialty Codes–creating major changes in the career paths of more than 32,000 airmen.” Whether or not the command structure already in place will transfer to NSA is unknown as of this writing. Nor is it clear whether AFCYBER’s offensive capability–real or imagined–will transfer to NSA. But with billions of dollars already spent on a score of top secret initiatives, included those hidden within Pentagon Special Access (SAP) or black programs, its a safe bet they will.

Defense analyst William M. Arkin points out in ***Code Names***, that these programs fall under the rubric of Special Technical Operations (STO). Arkin defines these as,

> Classified SAPs and other programs, weapons and operations associated with the CIA and “other government agencies.” Entire separate channels of communication and clearances exist to compartment these military versions of clandestine and covert operations involving special operations, paramilitary activity, covert action, and cyber-warfare. A STO “cell” exists in the Joint Chiefs of Staff and at most operational military commands to segregate STO activity from normal operational activity, even highly classified activity. (Code Names: Deciphering U.S. Military Plans, Programs, and Operations in the 9/11 World, Hanover, NH: Steerforth Press, 2005, p. 20)

Specific cyber-warfare programs identified by Arkin include the following: Adversary: an Air Force information warfare targeting system; Arena: an “object-based” simulation program to create “country studies of electronic infrastructure characteristics, targeting analyses, operational information warfare plans” as well as nearly *three dozen* other cyber-war programs and/or exercises.

Many of the Pentagon’s cyber-warfare initiatives flow directly from research conducted by the Defense Advanced Research Projects Agency (**DARPA**). For example, the agency’s

Information Processing Techniques Office (**IPTO**) has a brief to "create the advanced information processing and exploitation science, technologies, and systems for revolutionary improvements in capability across the spectrum of national security needs."

As can be seen from the brief survey above, the vast majority of Pentagon programs concern Cyber Command's *offensive* capability of which denial of service and other attacks against "adversaries" in the *heimat* are a distinct possibility. The *Journal* reports,

> The Department of Homeland Security is charged with securing the government's nonmilitary networks, and cybersecurity experts said the Obama administration will have to better define the extent of this military support to Homeland Security. "It's a fine line" between providing needed technical expertise to support federal agencies improving their own security and deeper, more invasive programs, said Amit Yoran, a former senior cybersecurity official at the Homeland Security Department. (Siobhan Gorman, "Gates to Nominate NSA Chief to Head New Cyber Command," The Wall Street Journal, April 24, 2009)

The Obama administration is expected to announce the the new agency's launch next week, after completing what it terms a "comprehensive review" in addition to recommendations for cybersecurity policy.

Geoff Morrell, a Pentagon spokesperson, told the *Journal* that Gates is "planning to make changes to our command structure to better reflect the increasing threat posed by cyber warfare," but "we have nothing to announce at this time." Morrell said the Department of Defense's 2010 budget proposal "calls for hiring hundreds more cybersecurity experts."

Aside from lining the pockets of enterprising grifters in the shadowy world populated by intelligence corporations, where top secret clearances are traded like highly-prized baseball cards, the potential for abuse by NSA given that agency's key role in illegal domestic surveillance raise the prospect of further entrenching the agency in our lives.

While Alexander sought to allay fears that NSA was out to run the nation's cybersecurity programs, he hastened to add that the agency's "tremendous technical capabilities" would be used to "assist" DHS in securing the government's civilian networks. But given AFCYBER's brief for offensive operations, what does this mean for civil liberties?

As *The New York Times* **reported** April 17, with NSA leading the charge to control "the government's rapidly growing cybersecurity programs," critics within the national security apparatus fear the move by Gates "could give the spy agency too much control over government computer networks." The *Times* avers,

> Rod Beckstrom, who resigned in March as director of the National Cyber Security Center at the Homeland Security Department, said in an interview that he feared that the N.S.A.'s push for a greater role in guarding the government's computer systems could give it the power to collect and analyze every e-mail message, text message and Google search conducted by every employee in every federal agency. (James Risen and Eric Lichtblau, "Control of Cybersecurity Becomes Divisive Issue," The New York Times, April 17, 2009)

This is hardly an issue that should only concern government insiders or those who engage in

bureaucratic in-fighting as if it were a blood sport. As a Pentagon agency, NSA has positioned itself to seize near total control over the country's electronic infrastructure, thereby exerting an intolerable influence–and chilling effect–over the nation's political life.

As we have seen in our recent history, NSA and their partners at CIA, FBI, et. al., have targeted political dissidents: to varying degrees, antiwar organizers, socialist, anarchist and environmental activists have fallen under NSA's electronic driftnet, most recently during last year's Republican National Convention.

As I **reported** last November, during the RNC conclave in St. Paul, Minnesota, local, state, federal officials as well as private security and telecommunications corporations conspired to target activists, journalists and concerned citizens during the so-called National Special Security Event.

The whistleblowing website *Wikileaks* published a leaked **planning document** which outlined the close coordination across multiple agencies, including the FBI, NSA, U.S. Northern Command and the National Geospatial-Intelligence Agency (NGA). Cell-phones and other electronic communications were routinely monitored in real-time and NGA provided detailed analysis derived from military spy satellites.

A "Strategic Vision" in the Service of Repression

Although the Air Force has lost out to NSA over control of Cyber Command, AFCYBER's **planning document** still provides a valuable glimpse into the formidable infrastructure arrayed against the American people.

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

And as "economic disparities" grow, particularly during a period of profound capitalist economic meltdown, newer and more effective measures to ensure compliance are required by the ruling class and its state. This is underscored by Cyber Command's 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)

As *Wired* defense analyst Noah Shachtman **wrote** last year,

> 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)

While the cut and color of the uniform may have changed under the Obama administration, placing Cyber Command under NSA's wing will almost certainly transform "cybersecurity" into a euphemism for *keeping the rabble in line*. Indeed, cybersecurity 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]

And when those "greater effects" are directed against American citizens theorized as "adversaries" by U.S. militarists and well-heeled corporate grifters, the problems posed by a panoptic surveillance state for a functioning democracy increase astronomically.

The already slim protections allegedly afforded by the shameful FISA Amendments Act have already been breeched by NSA. As *The New York Times* **reported** April 16, NSA interception of the private e-mail messages and phone calls of Americans have escalated "in recent months on a scale that went beyond the broad legal limits established by Congress last year."

As *Wired* **reported** April 17, the NSA isn't the only agency conducting cyber operations against American citizens. One of the FBI's International Terrorism Operations Sections requested an assist from the Bureau's Cryptographic and Electronic Analysis Unit, CEAU, according to **documents** obtained by the magazine under the Freedom of Information Act. The FBI "geek squad" was in a position to conduct a "remote computer attack" against the target, and that "they could assist with a wireless hack to obtain a file tree, but not the hard drive content."

This followed an April 16 **report** published by *Wired* that a "sophisticated FBI-produced spyware program has played a crucial behind-the-scenes role in federal investigations into extortion plots, terrorist threats and hacker attacks in cases stretching back at least seven years, newly declassified documents show."

But as I **documented** last year in a case involving activists targeted during anti-RNC protests, with "preemptive policing" all the rage in Washington, the same suite of hacking tools and spyware used to target criminals and terrorists are just as easily deployed against

political activists, particularly socialists, anarchists and environmental critics who challenge capitalism's free market paradigm.

Despite these revelations, the Obama administration is poised to hand control of the nation's electronic infrastructure over to an out-of-control agency riddled with corporate grifters and militarists whose bottom-line is not the security of the American people but rather, the preservation of an economically and morally bankrupt system of private profit fueled by wars of aggression and conquest.

Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and ***Global Research****, an independent research and media group of writers, scholars, journalists and activists based in Montreal, his articles can be read on* ***Dissident Voice****,* ***The Intelligence Daily****,* ***Pacific Free Press*** *and the whistleblowing website* ***Wikileaks****. 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/