GlobalResearch
Center for Research on Globalization

The Launching of U.S. Cyber Command (CYBERCOM).

Offensive Operations in Cyberspace

By Tom Burghardt
Global Research, July 01, 2009
Antifascist Calling... 30 June 2009

Region: USA
Theme: Police State & Civil Rights

U.S. Defense Secretary Robert Gates signed a memorandum on June 23 that announced the launch of U.S. Cyber Command (CYBERCOM). A scheme by securocrats in the works for several years, the order specifies that the new office will be a "subordinate unified command" under U.S. Strategic Command (STRATCOM).

According to the memorandum, CYBERCOM "will reach initial operating capability (IOC) not later than October 2009 and full operating capability (FOC) not later than October 2010."

Gates has recommended that this new Pentagon domain be led by Lt. General Keith Alexander, the current Director of the ultra-spooky National Security Agency (NSA). Under the proposal, Alexander would receive a fourth star and the new agency would be based at Ft. Meade, Maryland, NSA's headquarters.

Gates' memorandum specifies that CYBERCOM "must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners."

Ostensibly launched to protect military networks against malicious cyberattacks, the command's offensive nature is underlined by its role as STRATCOM's operational cyber wing. In addition to a defensive brief to "harden" the "dot-mil" domain, the Pentagon plan calls for an offensive capacity, one that will deploy cyber weapons against imperialism's adversaries.

One of ten Unified Combatant Commands, STRATCOM is the successor organization to Strategic Air Command (SAC). Charged with space operations (military satellites), information warfare, missile defense, global command and control, intelligence, surveillance and reconnaissance (ISR), as well as global strike and strategic deterrence (America's first-strike nuclear arsenal), it should be apparent that designating CYBERCOM a STRATCOM branch all but guarantees an aggressive posture.

As Antifascist Calling reported in May, the Pentagon's geek squad, the Defense Advanced Research Projects Agency (DARPA) is currently building a National Cyber Range (NCR), a test bed for developing, testing and fielding cyber weapons.

In conjunction with "private-sector partners," the agency averred in a January 2009 press release that NCR promises to deliver "'leap ahead' concepts and capabilities."

The Armed Forces Press Service reported June 24, that Pentagon Press Secretary Geoff Morrell told journalists that CYBERCOM is "not some sort of new and necessarily different authorities that have been granted." Obfuscating the offensive role envisaged for the command, Morrell told reporters: "This is about trying to figure out how we, within this department, within the United States military, can better coordinate the day-to-day defense, protection and operation of the department's computer networks."

Others within the defense bureaucracy are far more enthusiastic, and forthright, when it comes to recommending that cyber armaments be fielded as offensive weapons of war. Indeed, Armed Forces Journal featured a lengthy analysis advocating precisely that.

The world has abandoned a fortress mentality in the real world, and we need to move beyond it in cyberspace. America needs a network that can project power by building an af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack. (Col. Charles W. Williamson III, "Carpet Bombing in Cyberspace," Armed Forces Journal, May 2008)

We have heard these Orwellian arguments before; one can take it for granted that when militarists pontificate on the need for a "deterrent," the bombers are preparing for take off.

As with other Pentagon schemes, the technological quick fix may prove as deadly as the alleged threat, particularly where botnets are concerned.

A botnet is a collection of widely dispersed computers controlled from one or more central nodes. Often built by cyber criminals to implant malicious programs or code, steal passwords and other encrypted data from targeted systems, botnets are the bane of the Internet.

In these endeavors, sophisticated hackers are aided and abetted by the miserable security code or lax practices of Internet Service Providers (ISPs) more concerned with facilitating commerce–and the bottom line–than in providing adequate protection against criminals.

Indeed in March, the Electronic Privacy Information Center (EPIC) urged the Federal Trade Commission "to shut down Google's so-called cloud computing services, including Gmail and Google Docs, if the web giant can't ensure the safety of user data stored by these online apps," The Register reported.

EPIC's petition in part, was sparked "by a Google snafu that saw the company inadvertently share certain Google Docs files with users unauthorized to view them. Google estimates that the breach hit about 0.05 per cent of the documents stored by the service," according to The Register.

Infected computers are referred to as "zombies" that can be controlled remotely from any point on the planet by "master" machines. Unwary users are often "spoofed" by hackers through counterfeit e-mails replete with embedded hyperlinks into "cooperating" with the installation of malicious code.

While criminals employ botnets to generate spam or commit fraudulent transactions, draining a savings account or running-up credit card debt through multiple purchases for example, botnets also have the capacity to launch devastating distributed denial of service

(DDOS) attacks against inadequately defended computers or indeed, entire networks.

As many commentators have warned, the best defense is to write better security programs and exercise a modicum of common sense when using the Internet. The Pentagon however, has something else in mind.

Col. Williamson proposes to transform the Air Force's high-speed intrusion-detection systems into an offensive botnet by enabling "the thousands of computers the Air Force would normally discard every year for technology refresh, removing the power-hungry and heat-inducing hard drives, replacing them with low-power flash drives, then installing them in any available space every Air Force base can find." In other words, creating thousands of zombie machines.

"After that," Col. Williamson avers, "the Air Force could add botnet code to all its desktop computers attached to the Nonsecret Internet Protocol Network (NIPRNet). Once the system reaches a level of maturity, it can add other .mil computers, then .gov machines."

Underscoring the risks posed by out-of-control military hackers to hold America's, or any other nations' communications infrastructure hostage to a militarized state, Williamson suggests that in order to "generate the right amount of power for offense, all the available computers must be under the control of a single commander, even if he provides the capability for multiple theaters. While it cannot be segmented like an orange for individual theater commanders, it can certainly be placed under their tactical control." (emphasis added)

In other words, should an "individual theatre commander" desire to suddenly darken a city or wreck havoc on a nation's electrical infrastructure at the behest of his political masters then by all means, go right ahead! A proposal such as this, should it ever be implemented, would in essence, be a first-strike weapon.

Other plans for "defending" Pentagon computer networks are even more extreme.

STRATCOM commander Gen. Kevin Chilton has even suggested that "the White House retains the option to respond with physical force–potentially even using nuclear weapons–if a foreign entity conducts a disabling cyber attack against U.S. computer networks," according to a disturbing report published by Global Security Newswire. During a Defense Writers Group breakfast in May, Chilton told journalists:

"I think you don't take any response options off the table from an attack on the United States of America. Why would we constrain ourselves on how we respond?" …

Should the breaches evolve into more serious computer attacks against the United States, Chilton said he could not rule out the possibility of a military salvo against a nation like China, even though Beijing has nuclear arms. He rejected the idea that such a conflict would necessarily risk going nuclear.

"I don't think that's true," Chilton said.

At the same time, the general insisted that all strike options, including nuclear, would remain available to the commander in chief in defending the nation from cyber strikes.

“I think that’s been our policy on any attack on the United States of America,” Chilton said. “And I don’t see any reason to treat cyber any differently. I mean, why would we tie the president’s hands? I can’t. It’s up to the president to decide.” (Elaine M. Grossman, “U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber Attack,” Global Security Newswire, May 12, 2009)

While Pentagon spokesman Bryan Whitman told The New York Times that CYBERCOM’s launch “is not about the militarization of cyber,” how else can it be characterized?

Indeed, Whitman went on to say that CYBERCOM “is focused only on military networks to better consolidate and streamline Department of Defense capabilities into a single command.”

How then, should one interpret moves by the Pentagon to “consolidate and streamline” DoD “capabilities” under the purview of STRATCOM? Obviously, an entity defined as a “Unified Combatant Command” as clearly stated by General Chilton’s avowal to “leave all options on the table,” would combine cyber “defense” with STRATCOM’s global strike mission.

Antifascist Calling revealed last year, citing a U.S. Air Force planning document, that preparations are already underway to transform cyberspace into an offensive military domain. Indeed, Air Force theorists averred:

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. (Air Force Cyber Command, “Strategic Vision,” no date, emphasis added)

Echoing Air Force strategy, SecDef Gates memo clearly states, since “cyberspace and its associated technologies … are vital to our nation’s security,” the United States will “secure freedom of action in cyberspace” by standing-up a unified command “that possesses the required technical capability and remains focused on the integration of cyberspace operations.”

Simply put, the Pentagon intends to build an infrastructure fully-capable of committing high-tech war crimes.

Under NSA’s Operational Control

Meanwhile in the heimat, CYBERCOM will effectively be under the day-to-day control of the National Security Agency. This is hardly good news when it comes to civil liberties.

Leaving aside considerations of bureaucratic trench warfare with the Department of Homeland Security, charged with defending the state’s .gov and .com domains, the unprecedented power of CYBERCOM to conduct offensive military and surveillance operations within the United States itself is underlined by the preeminent role NSA will assume.

Authorized by the criminal Bush regime to carry out massive electronic surveillance of Americans' private communications in the wake of the 9/11 attacks, various driftnet spying operations continue under Obama's purported "change" administration. As Antifascist Calling has averred many times, the only "change" that's come to the White House has been the color of the drapes hanging in the Oval Office.

The New York Times revealed June 17, that the "National Security Agency is facing renewed scrutiny over the extent of its domestic surveillance program, with critics in Congress saying its recent intercepts of the private telephone calls and e-mail messages of Americans are broader than previously acknowledged." According to the Times, "The agency's monitoring of domestic e-mail messages, in particular, has posed longstanding legal and logistical difficulties, the officials said."

I take issue with the Times' characterization that such a breach of constitutional norms merely represent "logistical difficulties." As with a Times' report in April which alleged that NSA's driftnet spying under Obama was simply a problem of "overcollection," far from being mere technical issues, first and foremost, these violations represent political decisions made at the highest levels of the national security state itself.

Since April, when it was disclosed that the intercepts of some private communications of Americans went beyond legal limits in late 2008 and early 2009, several Congressional committees have been investigating. Those inquiries have led to concerns in Congress about the agency's ability to collect and read domestic e-mail messages of Americans on a widespread basis, officials said. Supporting that conclusion is the account of a former N.S.A. analyst who, in a series of interviews, described being trained in 2005 for a program in which the agency routinely examined large volumes of Americans' e-mail messages without court warrants. Two intelligence officials confirmed that the program was still in operation. (James Risen and Eric Lichtblau, "E-Mail Surveillance Renews Concerns in Congress," The New York Times, June 17, 2009)

Last year, congressional Democrats, including Senator now President, Obama, handed the NSA virtually unchecked power to spy on the private communications of Americans. In addition to granting retroactive immunity to telecom grifters who profited from their conspiracy to illegally spy on citizens for the state, the despicable FISA Amendments Act (FIA) gave NSA the legal cover to intercept Americans' communications "so long as it was done only as the incidental byproduct of investigating individuals 'reasonably believed' to be overseas," as the Times delicately put it.

CYBERCOM's brief, and its deployment inside NSA with full access to the agency's powerful computing assets, and with a mission to conduct global Intelligence, Surveillance and Reconnaissance (ISR) at the behest of their STRATCOM masters, mean that despite bromides about "privacy concerns," the Pentagon will most assuredly be interested in developing an attack matrix that can just as easily be turned inward. After all as General Chilton asserts, "it's up to the president to decide."

"One thing that is pretty clear," Wired reports, "NSA will be leading this emerging command." Indeed, NSA "may also come to dominate the wider government cyber defense effort, as well." As The Wall Street Journal revealed, the Defense Department's 2010 budget "envisions training and graduating more than 200 cyber-security officers annually." In contradistinction to DoD, "the Department of Homeland Security has 100 employees dedicated to civilian cyber security, with plans to reach 260 next year," the Journal reports.

In other words, right from the get-go NSA will be assuming operational control of CYBERCOM. This is driven home by the fact that the Pentagon is already receiving the vast majority of appropriations for state cybersecurity initiatives and have thousands of cyberwarriors across all branches of the military, including outsourced private contractors who labor for DoD, ready, willing and able to staff the new command.

As Antifascist Calling revealed in April, with billions of dollars already spent on a score of top secret cyber initiatives, including those hidden within Pentagon Special Access or black programs, the issue of oversight is already a moot point.

Defense analyst William M. Arkin in his essential book, Code Names, described some three dozen cyberwar programs and/or exercises, currently being pursued by the Pentagon. Since the book's 2005 publication, many others undoubtedly have come on-line.

While NSA Director Alexander has explicitly stated that he does "not want [NSA] to run cybersecurity for the United States government," CYBERCOM's stand-up, and Alexander's near certain appointment as commander, all but guarantees that the agency will be a ubiquitous and silent gatekeeper answerable to no one.

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, 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.*
