GlobalResearch
Center for Research on Globalization

Cyber Command Prepares for High-Tech War Crimes: “Computer Network Attacks to Protect U.S. Interests”

By Tom Burghardt
Global Research, November 14, 2010
Antifascist Calling... 14 November 2010
Theme: Intelligence, Police State & Civil Rights

While a bureaucratic turf war rages between the CIA and U.S. Cyber Command (CYBERCOM) over which secret state agency will be authorized to launch network attacks outside a “war zone,” the big losers, as always, will be those unfortunate enough to find themselves on the receiving end of a military-grade “logic bomb.”

Last week, The Washington Post reported that CYBERCOM “is seeking authority to carry out computer network attacks around the globe to protect U.S. interests.” Leaving aside the thorny question of whose interests are being “protected” here, the Post tells us that unnamed administration lawyers are “uncertain about the legality of offensive operations.”

Coming from a government that’s incorporated the worst features of the previous regime into their repertoire, that’s rather rich.

“The CIA has argued,” the Post informs, “that such action is covert, which is traditionally its turf.” Pentagon thrill-kill specialists beg to differ, asserting that “offensive operations are the province of the military and are part of its mission to counter terrorism, especially when, as one official put it, ‘al-Qaeda is everywhere’.”

That certainly covers a lot of ground! As a practical matter it also serves as a convenient justification–or pretext, take your pick–for our minders in Ft. Meade, Langley or Cheltenham to consummate much in the mischief department.

And with alarmist media reports bombarding us every day with dire scenarios, reminiscent of the “weapons of mass destruction” spook show that preceded the Iraq invasion, where China, Iran, Russia and North Korea are now stand-ins for “Saddam” in the cyberwar Kabuki dance, it is hardly surprising that “liberal” Democrats and “conservative” Republicans are marching in lockstep.

InfoSecurity reported last week that during a recent Manhattan conference, Rep. Yvette Clarke (D-NY) proclaimed that “the likelihood of a cyberattack that could bring down our [electrical] grid is … 100%. Our networks are already being penetrated as we stand here. We are already under attack. We must stop asking ourselves ‘could this happen to us’ and move to a default posture that acknowledges this fact and instead asks ‘what can we do to protect ourselves’?”

Why cede even more control to the secret state and their corporate partners who stand to make a bundle in the latest iteration of the endless “War on Terror” (Cyber Edition), of

course!

An Offensive Brief

Despite all the hot air about protecting critical infrastructure and the mil.com domain, the offensive nature of Pentagon planning is written into Cyber Command's DNA.

As Antifascist Calling reported in April, the organization's aggressive posture is writ large in several Air Force planning documents. In a 2006 presentation to the Air Force Cyber Task Force for example, A Warfighting Domain: Cyberspace, Dr. Lani Kass asserted that "Cyber is a war-fighting domain. The electromagnetic spectrum is the maneuver space. Cyber is the United States' Center of Gravity–the hub of all power and movement, upon which everything else depends. It is the Nation's neural network."

Kass averred that "Cyber superiority is the prerequisite to effective operations across all strategic and operational domains–securing freedom from attack and freedom to attack."

Accordingly, she informed her audience that "Cyber favors the offensive," and that the transformation of the electromagnetic spectrum into a "warfighting domain" will be accomplished by: "Strategic Attack directly at enemy centers of gravity; Suppression of Enemy Cyber Defenses; Offensive Counter Cyber; Defensive Counter Cyber; Interdiction."

Two years later, the Strategic Vision unveiled by the Air Force disclosed that the purpose for standing up a dedicated cyber command is to "deceive, deny, disrupt, degrade, and destroy" an adversary's information infrastructure.

Air Force theorists averred that since "the confluence of globalization, economic disparities, and competition for scarce resources" pose significant challenges for the U.S. Empire, all the more pressing in light of capitalism's on-going economic crisis, an offensive cyber posture must move rapidly beyond the theoretical plane.

Echoing Kass, and in order to get a leg-up on the competition, we were told that "controlling cyberspace is the prerequisite to effective operations across all strategic and operational domains–securing freedom from attack and freedom to attack."

Shortly thereafter, Air Force Col. Charles W. Williamson III wrote in the prestigious Armed Forces Journal that "America needs the ability to carpet bomb in cyberspace to create the deterrent we lack." Williamson averred that "America must have a powerful, flexible deterrent that can reach far outside our fortresses and strike the enemy while he is still on the move."

His solution? Create a military-grade botnet that marshals the computing power of tens of thousands of Defense Department machines. "To generate the right amount of power for offense," Williamson wrote, "all the available computers must be under the control of a single commander, even if he provides the capability for multiple theaters."

And if innocent parties, not to mention a potential adversary's civilian infrastructure is destroyed in the process, Williamson declares that "if the botnet is used in a strictly offensive manner, civilian computers may be attacked, but only if the enemy compels us."

Indeed, "if the U.S. is defending itself against an attack that originates from a computer

which was co-opted by an attacker, then there are real questions about whether the owner of that computer is truly innocent."

But as we know from observing the conduct of the U.S. military in Iraq and Afghanistan, outside the imperial blast walls no one is "truly innocent."

While the Air Force may have lost the intramural skirmish to run the organization, a task now shared amongst the other armed services and NSA, their preemptive war doctrines are firmly in place. And with an operating budget of $120 million this year, to increase to $150 million in fiscal year 2011, excluding of course highly-secretive Special Access Programs hidden deep inside the Pentagon's "black" budget, it's off to the races.

As I reported last year, when Secretary of Defense Robert M. Gates penned a Memorandum that marked its official launch, the former CIA chief and Iran-Contra criminal specified that CYBERCOM would be a "subordinate unified command" under U.S. Strategic Command (STRATCOM).

As readers are well aware, STRATCOM is the Pentagon satrapy charged with running space operations, information warfare, missile defense, global command, control, intelligence, surveillance and reconnaissance (C4ISR), global strike and strategic deterrence; in other words, they're the trigger finger on America's first-strike nuclear arsenal.

A Strategic Command Fact Sheet published in June told us that Cyber Command "plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

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

What form that "support" will take is clear from previous agreements between the U.S. secret state and their "international partners." Beneath the dark banner of the UK-USA Security Agreement that powers the ECHELON signals intelligence (SIGINT) collection and analysis network, agencies such as NSA and Britain's Government Communications Headquarters (GCHQ) keep a watchful eye on global communications.

On the domestic front, as I reported last month, a Memorandum of Agreement forged between the Department of Homeland Security and the National Security Agency means that "protecting" critical civilian infrastructure and communications assets, including the internet, is for all practical purposes now part of the Pentagon's cyberwar brief.

With authority to troll our communications handed to NSA by the Bush and Obama administrations under top secret provisions of the Comprehensive National Cybersecurity Initiative (CNCI), the American people have no way of knowing what cybersecurity programs exist, who decides what is "actionable intelligence," or where private communications land after becoming part of the "critical infrastructure and key resources" landscape.

And with civilian control over "black" Pentagon programs off the table since the darkest days of the Cold War, the Defense Department's announcement last week that Cyber

Command has achieved “full operational capability” should give pause.

Long-Running Feud

War criminal, arch geopolitical manipulator and corporate bag man Henry Kissinger once famously said, “covert action should not be confused with missionary work.”

While true as far as it goes, bureaucratic blood-sport between the CIA and the Defense Department over control of world-wide cyber operations reflects a long-running battle within the secret state over which covert branch of government will command resources and run clandestine programs across the global “War on Terror” landscape.

Currently in the driver’s seat when it comes to the deadly drone war in Pakistan and protecting America’s opium-growing and heroin-dealing regional allies, the Agency vigorously objects to Pentagon maneuvers to carry out offensive cyber operations away from acknowledged war zones, because, so goes the argument, they have exclusive rights to the covert action brief.

Such claims have been challenged by the Pentagon, and considering the formidable assets possessed by Cyber Command and NSA, the Agency is likely to lose out when the Obama regime issues a ruling later this year.

This raises an inevitable question, not that its being asked by congressional grifters or corporate media stenographers: should NSA, the Pentagon or indeed any other secret state agency, including the CIA, be tasked with cybersecurity generally, let alone given carte blanche to conduct clandestine and legally dubious missions inside our computer networks?

As security expert Bruce Schneier wrote last year, “Cybersecurity isn’t a military problem.” In fact when the Bush and Obama governments gave the Pentagon a free hand to driftnet spy on the American people, Schneier averred that programs like the NSA’s warrantless wiretapping program “created additional vulnerabilities in our domestic telephone networks.”

Vulnerabilities not likely to be addressed by administration proposals that would further weaken encryption standards and order telecommunications and computer manufacturers to build surveillance-ready backdoors into their devices and networks, as The New York Times disclosed in September.

Despite a warning last year by former DHS National Cyber Security division head Amit Yoran that “the intelligence community has always and will always prioritize its own collection efforts over the defensive and protection mission of our government’s and nation’s digital systems,” the securitization of America’s electronic networks is proceeding at break-neck speed.

Describing the military’s power-grab in benign terms, NSA/CYBERCOM director Alexander characterized Pentagon operational plans as an “active defense,” one that “hunts” inside a computer network “for malicious software, which some experts say is difficult to do in open networks and would raise privacy concerns if the government were to do it in the private sector,” The Washington Post reports.

An unnamed “senior defense official” described the process as an “ability to push ‘out as far as we can’ beyond the network perimeter to ‘where the threat is coming from’ in order to

eliminate it."

Never mind that pushing out "as far as we can" will mean that the American people will be subject to additional constitutional breaches or that current Pentagon initiatives, such as NSA's warrantless wiretapping programs are not subject to meaningful public oversight and are hidden beneath top secret layers of classification and the continual invocation of the "state secrets" privilege by the Bush and Obama administrations.

Regardless of which secret state agency comes out on top in the current dispute, where choosing between the CIA and the Pentagon offers a Hobson's choice of whether one prefers to be poisoned or shot, as Doug Henwood points wrote in Left Business Observer following the mid-term elections: "A country that's rotting from the head, poisoned by alienation, plutocracy, and an aversion to thinking, careens from one idiocy to another."

And so it goes, on and on...

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, Uncommon Thought Journal, and the whistleblowing website WikiLeaks. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by AK Press and has contributed to the new book from Global Research, The Global Economic Crisis: The Great Depression of the XXI Century.

The original source of this article is Antifascist Calling...
Copyright © Tom Burghardt, Antifascist Calling..., 2010

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca