Cyberwar, the Internet and the Militarization of Civil Society

By Tom Burghardt
Global Research, October 28, 2013
Antifascist Calling and Global Research 25 April 2010

Region: USA
Theme: Intelligence, Police State & Civil Rights

This April 2010 path breaking article foresaw what is now unfolding in front of our very eyes: the repeal of civil liberties, privacy and personal freedoms, war without borders internationally...

Unfailingly, defense industry boosters and corporate media acolytes promote the disturbing hypothesis annunciated by former Director of National Intelligence, Mike McConnell, that the nation is in peril.

In a February Washington Post op-ed, the latest version of the "grave and gathering danger" big lie repeated endlessly by former President Bush during the run-up to the Iraq invasion, McConnell claims that "the United States is fighting a cyber-war today, and we are losing."

Since leaving the secret state's employ, McConnell returned to his old beltway bandit firm, Booz Allen Hamilton, as a senior vice president in charge of the company's national security business unit, a position he held after "retiring" as Director of the National Security Agency back in 1996.

Critics, including security system design experts and investigative journalists, question the alarmist drumbeat that promises to dump tens of billions of federal dollars into the coffers of firms like McConnell's.

Indeed, Washington Technology reported two weeks ago that Booz Allen Hamilton landed a $20M contract to "foster collaboration among telecommunications researchers, University of Maryland faculty members and other academic institutions to improve secure networking and telecommunications and boost information assurance."

While we're at it, let's consider the deal that L-3 Communications grabbed from the Air Force just this week. Washington Technology reports that L-3, No. 8 on that publication's "2009 Top Ten" list of federal prime contractors, "will assist the Air Forces Central Command in protecting the security of its network operations under a contract potentially worth $152 million over five years."

Or meditate on the fact that security giant Raytheon's soaring first quarter profits were due to the "U.S. military demand for surveillance equipment and new ways to prepare soldiers for wars," MarketWatch reported Thursday.

Chump-change perhaps in the wider scheme of things, considering America's nearly $800B defense budget for FY2011, but fear sells and what could be more promising for enterprising

security grifters than hawking terror that comes with the threat that shadowy “asymmetric” warriors will suddenly switch everything off?

As Bloomberg News disclosed back in 2008, both Lockheed Martin and Boeing “are deploying forces and resources to a new battlefield: cyberspace.”

As journalist Gopal Ratnam averred, the military contractors and the wider defense industry are “eager to capture a share of a market that may reach $11 billion in 2013,” and “have formed new business units to tap increased spending to protect U.S. government computers from attack.”

Linda Gooden, executive vice president of Lockheed’s Information Systems & Global Services unit told Bloomberg, “The whole area of cyber is probably one of the faster-growing areas” of the U.S. budget. “It’s something that we’re very focused on.”

Lockheed’s close, long-standing ties with the National Security Agency all but guarantee a leg up for the firm as it seeks to capture a large slice of the CYBERCOM pie.

The problem with a line of reasoning that U.S. efforts are primarily concerned with defending Pentagon networks reveals a glaring fact (largely omitted from media accounts) that it is the Pentagon, and not a motley crew of hackers, cyber-criminals or “rogue states” that are setting up a formidable infrastructure for launching future high-tech war crimes.

This is clearly spelled out in the DOD’s 2010 Quadrennial Defense Review (QDR). In that document Pentagon planners aver that CYBERCOM “will direct the operation and defense of DOD’s information networks, and will prepare to, and when directed, conduct full spectrum cyberspace military operations. An operational USCYBERCOM will also play a leading role in helping to integrate cyber operations into operational and contingency planning.”

The QDR promises to stand-up “10 space and cyberspace wings” within the Department of the Air Force that will work in tandem with Cyber Command.

Last week, Antifascist Calling reported how the mission of that Pentagon Command is primarily concerned with waging offensive operations against “adversaries” and that civilian infrastructure is viewed as a “legitimate” target for attack.

In that piece, I cited documents released by the Senate Armed Services Committee (SASC), publicly available, though buried within a mass of Broad Agency Announcements, that solicited bids for contracts by the various armed service branches from private defense and security corporations for the design of offensive cyber weapons.

Accordingly, the Air Force Research Laboratory-Rome issued a Broad Agency Announcement (BAA-10-04-RIKA) February 25, for “Full Spectrum Cyber Operations Technology” that will address issues related to “the integration and better coordination of the day-to-day defense, protection, and operation of DoD networks as well as the capability to conduct full spectrum cyberspace military operations.”

The BAA explicitly states that “research efforts under this program are expected to result in functional capabilities, concepts, theory, and applications ideally addressing cyber operations problems including projects specializing in highly novel and interesting applicable technique concepts will also be considered, if deemed to be of ‘breakthrough’ quality and importance.”

Unsurprisingly, “technical information relevant to potential submitters is contained in a classified addendum at the Secret level to this BAA.”

But the military aren’t the only players leading the charge towards the development of highly-destructive cyberweapons. Indeed, the Cyber Conflict Research Studies Association (CCSA), a Washington, D.C. based think tank is top-heavy with former intelligence, military and corporate officials doing just that.

The group’s board of directors are flush with former officers or consultants from the FBI, Defense Intelligence Agency (DIA), the Air Force, National Security Agency, Department of Homeland Security and the CIA. Other board members are top officers in the spooky “public-private” FBI-affiliated spy outfit InfraGard, the Council on Foreign Relations as well as high-powered firms such as General Dynamics, Science Applications International Corporation (SAIC) and Goldman Sachs.

Demonstrating the interconnected nature of domestic surveillance, repression and military cyberwar operations, CCSA’s Treasurer, Robert Schmidt, is currently a member of the Office of the Director of National Intelligence, Council on Domestic Intelligence and the secretive Intelligence and National Security Association (INSA). Additionally, Schmidt is the President/CEO of InfraGard and “leads the operational side of private sector involvement with the Federal Bureau of Investigation’s InfraGard program.” How’s that for a hat trick!

What that “operational side” entails has never been publicly disclosed by the organization, but as I wrote back in 2008, citing Matthew Rothschild’s chilling piece in The Progressive, martial law is high on InfraGard’s agenda.

Members on CCSA’s board of directors, like others whirling through the revolving door between government and the private sector were/are officers or consultants to the FBI, NSA, DHS and other secret state intelligence agencies. Others were/are key advisers on the National Security Council or serve as consultants to industry-sponsored associations such as the Armed Forces Communications and Electronics Association (AFCEA) and INSA.

Dovetailing with research conducted by the Pentagon and their Intelligence Community partners, one CCSA study will explore “the full spectrum of military computer network operations, defined as computer network defense (CND), computer network exploit (CNE) and computer network attack (CNA), and examines the potential synergies and tradeoffs between those three categories.”

As befitting research conducted by the Military-Industrial-Security-Complex (MISC), CCSA’s study “will involve key academicians, strategists, military and intelligence community leaders and operational cyber practitioners to analyze key dilemmas of doctrine, organization, training, and planning, particularly with respect to integrating cyber warfare capabilities with kinetic operations.”

Key questions to be answered, among others, include “How can cyberwarfare capabilities be best integrated with other military forces?” and “How can leaders and personnel for conducting cyberwarfare be trained, educated and grown?”

Clearly, these are not academic issues.

DARPA to the Rescue

The Pentagon's "blue sky" research arm, the Defense Advanced Research Projects Agency (DARPA) is chock-a-block with programs investigating everything from Neurotechnology for Intelligence Analysts to Operationally-Focused Systems Integration (OFSI) "that align DARPA technologies with explicit opportunities for military operational impact."

Certainly, given the precarious state of the global capitalist economy, the enfeebled nature of American democratic institutions, and with no end in sight to planet-wide imperial adventures to secure access to increasingly shrinking energy reserves and other strategic resources, technological "silver bullets" are highly sought-after commodities by corporate and military bureaucracies. Such technophilic preoccupations by the MISC all but guarantee that the "state of exception" inaugurated by the 9/11 provocation will remain a permanent feature of daily life.

Several, interrelated DARPA projects feed into wider Pentagon cyberwar research conducted by the Army, Navy and Air Force.

One component of this research is DARPA's National Cyber Range (NCR). The brainchild of the agency's Strategic Technical Office (STO), NCR is conceived as "DARPA's contribution to the new federal Comprehensive National Cyber Initiative (CNCI), providing a 'test bed' to produce qualitative and quantitative assessments of the Nation's cyber research and development technologies."

While DARPA claims that it is "creating the National Cyber Range to protect and defend the nation's critical information systems," a "key vision" behind the program "is to revolutionize the state of the art of test range resource and test automation execution."

While short on specifics, DARPA's "vision of the NCR is to create a national asset for use across the federal government to test a full spectrum of cyber programs."

Many of the military programs slated for testing at NCR are highly classified, including those that fall under the purview of Pentagon Special Access or black programs. As defense analyst William M. Arkin pointed out in Code Names, such programs are hidden under the rubric of Special Technical Operations that have their own "entire separate channels of communication and clearances." STO's "exist to compartment these military versions of clandestine and covert operations involving special operations, paramilitary activity, covert action, and cyber-warfare." Arkin identified nearly three dozen cyberwar programs or exercises back in 2005; undoubtedly many more have since come online.

As Aviation Week reported in 2009, "Devices to launch and control cyber, electronic and information attacks are being tested and refined by the U.S. military and industry in preparation for moving out of the laboratory and into the warfighter's backpack."

But as "with all DARPA programs," the agency "will transition the operation of the NCR at a later date to an operational partner. No decision has been made on who will operate the final range."

Amongst the private defense, security and academic "partners" involved in NCR's development are the usual suspects: scandal-tainted BAE Systems; General Dynamics-Advanced Information Systems; Johns Hopkins University Applied Physics Laboratory; Lockheed Martin; Northrop Grumman-Intelligence, Surveillance and Reconnaissance Systems Division; Science Applications International Corporation; and SPARTA.

The aggressive nature of what has since evolved into CYBERCOM is underscored by several planning documents released by the U.S. Air Force. In a 2006 presentation to the Air Force Cyber Task Force, A Warfighting Domain: Cyberspace, Dr. Lani Kass unabashedly asserts: "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 Air Force 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."

While the Pentagon and their embedded acolytes in academia, the media and amongst corporate grifters who stand to secure billions in contracts have framed CYBERCOM's launch purely as a defensive move to deter what Wired investigative journalist Ryan Singel has denounced as "Cyberarmaggedon!" hype to protect America's "cyber assets" from attack by rogue hackers, states, or free-floating terrorist practitioners of "asymmetric war," CYBERCOM's defensive brief is way down the food chain.

Indeed, "options for the Operational Command for Cyberspace" include the "scalability of force packages" and their "ease of implementation" and, as I wrote last week citing but two of the fourteen examples cited by the Senate, "research, development, and acquisition" of cyber weapons. This is attack, not defense mode.

Americans' Privacy: a Thing of the Past

Situating CYBERCOM under the dark wings of U.S. Strategic Command and the National Security Agency, is a disaster waiting to happen.

As we now know, since 2001 NSA under dubious Office of Legal Counsel (OLC) findings that are still classified, and the despicable 2008 FISA Amendments Act, the Executive Branch was handed the authority the spy on American citizens and legal residents with impunity.

During his confirmation hearing as Cyber Command chief on April 15, NSA Director Lt. General Keith Alexander sought to assure the Senate Armed Services Committee (SASC) that "this is not about the intent to militarize cyber-space. My main focus is on building the capacity to secure the military's operational networks."

He told the Senate panel that if called in to help protect civilian networks, both NSA and Cyber Command "will have unwavering dedication to the privacy of American citizens."

Alexander was far cagier however in his written responses in a set of Advanced Questions posed by the SASC.

While corporate media like the dutiful stenographers they are, repeated standard Pentagon boilerplate that the secret state has an "unwavering dedication" to Americans' privacy, the Electronic Privacy Information Center (EPIC) filed a Freedom of Information Act request demanding answers and the release of the classified supplement.

Alexander stated in his written testimony that although "U.S. Cyber Command's mission will

not include defense of the .gov and .com domains, given the integration of cyberspace into the operation of much of our critical infrastructure and the conduct of commerce and governance, it is the obligation of the Department to be prepared to provide military options to the President and SECDEF if our national security is threatened."

He also defended the statement that "DOD's mission to defend the nation 'takes primacy' over the Department of Homeland Security's role in some situations."

"Of greater concern" EPIC wrote in their brief, "may be the questions that Lt. Gen. Alexander chose to respond to in classified form. When asked if the American people are 'likely to accept deployment of classified methods of monitoring electronic communications to defend the government and critical infrastructure without explaining basic aspects of how this monitoring will be conducted and how it may affect them,' the Director acknowledged that the Department had a 'need to be transparent and communicate to the American people about our objectives to address the national security threat to our nation–the nature of the threat, our overall approach, and the roles and responsibilities of each department and agency involved–including NSA and the Department of Defense,' but then chose include that the rest of his response to that question in the 'classified supplement'."

"Most troubling of all" EPIC averred "is the classified nature of the responses to advance questions 27b) and 27c). After responding to the question of how the internet could be designed differently to provide greater inherent security by describing vague 'technological enhancements' that could enhance mobility and possibly security, Lt. Gen. Alexander responded to 'Is it practical to consider adopting those modifications?' and 'What would the impact be on privacy, both pro and con?' by referring the Senators to the 'classified supplement.' No answer to either question was provided in the public record."

But in considering these questions, perhaps the SASC should have referred to ex-spook McConnell's February Washington Post op-ed: "More specifically, we need to reengineer the Internet to make [it] more manageable. The technologies are already available from public and private sources and can be further developed if we have the will to build them into our systems and to work with our allies and trading partners so they will do the same."

Is this a great country, or what!

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