GlobalResearch
Center for Research on Globalization

Cyberspace, the Battlefield of the Future: Pentagon Ramps-Up Cyberwar Plans

By Tom Burghardt
Global Research, June 13, 2011
Antifascist Calling... 13 June 2011

Region: USA
Theme: Police State & Civil Rights

As the Obama administration expands Bush-era surveillance programs over the nation's electronic communications' infrastructure, recent media reports provide tantalizing hints of Pentagon plans for waging cyberwar against imperialism's geopolitical rivals.

On May 31, *The Wall Street Journal* disclosed that the Pentagon now asserts "that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force."

One sound bite savvy wag told journalist Siobhan Gorman, "if you shut down our power grid, maybe we will put a missile down one of your smokestacks."

Also on May 31, *The Washington Post* reported that America's shadow warriors have "developed a list of cyber-weapons and -tools, including viruses that can sabotage an adversary's critical networks, to streamline how the United States engages in computer warfare."

That "classified list of capabilities has been in use for several months," with the approval of "other agencies, including the CIA." *Post* reporter Ellen Nakashima informed us that this "sensitive program … forms part of the Pentagon's set of approved weapons or 'fires' that can be employed against an enemy."

Not to be left in the dust by their U.S. and Israeli allies, *The Guardian* reported that the "UK is developing a cyber-weapons programme that will give ministers an attacking capability to help counter growing threats to national security from cyberspace."

Armed Forces Minister Nick Harvey told *The Guardian* that "action in cyberspace will form part of the future battlefield" and will become "an integral part of the country's armoury."

It appears that Western military establishments are in the grips of a full-blown cyber panic or, more likely, beating the war drums as they roll out new product lines with encouragement from corporate partners eager to make billions developing new weapons systems for their respective political masters.

And why not? As *Bloomberg News* reported back in 2008, both Lockheed Martin and Boeing "are deploying forces and resources to a new battlefield: cyberspace."

Bloomberg averred that 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."

As part of the new strategy to be released later this month, the *Post* reports that the military needs "presidential authorization to penetrate a foreign computer network and leave a cyber-virus that can be activated later."

However, when it comes to espionage or other activities loudly denounced as illegal intrusions into the sacrosanct world of government and corporate crime and corruption, the "military does not need such approval."

We're told such "benign" activities "include studying the cyber-capabilities of adversaries or examining how power plants or other networks operate."

"Military cyber-warriors," Nakashima writes, "can also, without presidential authorization, leave beacons to mark spots for later targeting by viruses," an "unnamed military official" told the *Post*.

But wait, aren't those *precisely* the types of covert actions decried by politicians, media commentators and assorted experts when they're directed against the *heimat*? Is there a double standard here? Well, of course there is!

Along with a flurry of Defense Department leaks designed to ratchet-up the fear factor and lay the groundwork for billions more from Congress for giant defense firms servicing the Pentagon's unquenchable thirst for ever-deadlier weapons systems–cyber, or otherwise–"threat inflation" scaremongering described by researchers Jerry Brito and Tate Watkins in their essential paper, *Loving the Cyber Bomb?*, take center stage.

Just last week, former Democratic party congressional hack, current CIA Director and Obama's nominee to lead the Defense Department, Leon Panetta, told the Senate Armed Services Committee that "the next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems," *The Christian Science Monitor* reported.

Cripple the financial system? Why greedy banksters and corporate bottom-feeders seem to be doing a splendid job of it on their own without an assist from shadowy Russian hackers, the People's Liberation Army or LulzSec pranksters!

However, the Pentagon's propaganda blitz (courtesy of a gullible or complicitous corporate media, take your pick) is neither meant to inform nor educate the public but rather, to conceal an essential fact: the United States is *already* engaged in hostile cyber operations against their geopolitical rivals–and allies–and have been doing so since the 1990s, if not earlier, as journalist Nicky Hager revealed when he blew the lid off NSA's Echelon program in a 1997 piece for *CovertAction Quarterly*.

Botnets and Root Kits: What the HBGary Hack Revealed

When *The Wall Street Journal* informed readers that the "Pentagon's first formal cyber strategy … represents an early attempt to grapple with a changing world in which a hacker

could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military," what the *Journal* didn't disclose is that the Defense Department is seeking the technological means to do just that.

Implying that hacking might soon constitute an "act of war" worthy of a "shock and awe" campaign, never mind that attributing an attack by a criminal or a state is no simple matter, where would the Pentagon draw the line?

After all as *The Guardian* reported, with the "underground world of computer hackers … so thoroughly infiltrated in the US by the FBI and secret service," will some enterprising criminal acting as a catspaw for his/her U.S. handlers, gin-up an incident thereby creating Panetta's "cyber Pearl Harbor" as a pretext for a new resource war?

While fanciful perhaps, if recent history is any guide to future American actions (can you say "Iraq" and "weapons of mass destruction"), such fabrications would have very deadly consequences for those on the wrong side of this, or some future, U.S. administration.

But we needn't speculate on what the Pentagon *might* do; let's turn our attention instead to what we know they're doing already.

Back in February, *The Tech Herald* revealed that the private security firms HBGary Federal, HBGary, Palantir Technologies and Berico Technologies were contacted by the white shoe law firm Hunton & Williams on behalf of corporate clients, Bank of America and the U.S. Chamber on Commerce, to "develop a strategic plan of attack against Wikileaks."

The scheme concocted by "Team Themis" was to have included a dirty tricks campaign targeting journalists, WikiLeaks supporters, their *families* and the whistleblowing group itself through "cyber attacks, disinformation, and other potential proactive tactics."

But when the CEO of HBGary Federal boasted to the *Financial Times* that he had penetrated the cyber-guerrilla collective Anonymous, the group struck back and pwned ("owned") HBGary's allegedly "secure" servers, seizing a treasure trove of some 70,000 internal emails and other documents, posting them on the internet.

As I reported earlier this year, Team Themis looked like a smart bet. After all, HBGary and the other firms touted themselves as "experts in threat intelligence and open source analysis" with a focus on "Information Operations (INFOOPS); influence operations, social media exploitation, new media development."

Palantir, which was fronted millions of dollars by the CIA's venture capitalist arm, In-Q-Tel, bragged that they could deliver "the only platform that can be used at the strategic, operational, and tactical levels within the US Intelligence, Defense, and Law Enforcement Communities," and that they can draw "in any type of data, such as unstructured message traffic, structured identity data, link charts, spreadsheets, SIGINT, ELINT, IMINT and documents."

In other words, these firms subsisted almost entirely on U.S. government contracts and, in close partnership with mega-giant defense companies such as General Dynamics, SRA International, ManTech International and QinetiQ North America, were actively building cyber weapons for the Defense Department.

In the aftermath of the HBGary sting, investigative journalist Nate Anderson published an essential piece for *Ars Technica* which described how HBGary and other firms were writing "backdoors for the government."

"In 2009," Anderson wrote, "HBGary had partnered with the Advanced Information Systems group of defense contractor General Dynamics to work on a project euphemistically known as 'Task B.' The team had a simple mission: slip a piece of stealth software onto a target laptop without the owner's knowledge."

HBGary's CEO Greg Hoglund's "special interest," Anderson reported, "was in all-but-undetectable computer 'rootkits,' programs that provide privileged access to a computer's innermost workings while cloaking themselves even from standard operating system functions. A good rootkit can be almost impossible to remove from a running machine–if you could even find it in the first place."

The secret-shredding web site Public Intelligence published HBGary's 2008 paper, Windows Rootkit Analysis Report. Amongst the nuggets buried within its 243 pages we learned that Hoglund suggested to his secret state and corporate clients that "combining deployment of a rootkit with a BOT makes for a very stealth piece of malicious software."

Readers should recall that back in 2008, an article published in the influential *Armed Forces Journal* advocated precisely that.

Col. Charles W. Williamson III's piece, "Carpet Bombing in Cyberspace," advocated "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."

It would appear that the project envisioned by HBGary and General Dynamics would combine the stealthy features of a rootkit along with the destructive capabilities of a botnet.

One can only presume that defense firms are building malware and other attack tools for the Defense Department, the CIA, the National Security Agency and USCYBERCOM, and that they constitute the short list of "approved weapons or 'fires'" alluded to by *The Washington Post*.

A 2009 HBGary contract proposal released by Public Intelligence, DoD Cyber Warfare Support Work Statement, disclosed that the "contract will include efforts to examine the architecture, engineering, functionality, interface and interoperability of Cyber Warfare systems, services and capabilities at the tactical, operational and strategic levels, to include all enabling technologies."

The firm proposed an "operational exercise design and construction," as well as "operations and requirements analysis, concept formulation and development, feasibility demonstrations and operational support."

"This will include," the proposal averred, "efforts to analyze and engineer operational, functional and system requirements in order to establish national, theater and force level architecture and engineering plans, interface and systems specifications and definitions, implementation, including hardware acquisition for turnkey systems."

Under terms of the contract, the company will "perform analyses of existing and emerging

Operational and Functional Requirements at the force, theater, Combatant Commands (COCOM) and national levels to support the formulation, development and assessment of doctrine, strategy, plans, concepts of operations, and tactics, techniques and procedures in order to provide the full spectrum of Cyber Warfare and enabling capabilities to the warfighter."

In fact, during an early roll-out of the Pentagon's cyber panic product line five years ago, Dr. Lani Kass, a former Israeli Air Force major and acolyte of neocon war criminals Dick Cheney and Donald Rumsfeld, and who directs the Air Force Cyber Space Task Force under Bush and Obama, submitted a provocative proposal.

During a 2006 presentation titled, A Warfighting Domain: Cyberspace, Kass asserted that "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 a militarized internet 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."

In the years since that presentation such plans are well underway.

In another leaked file, Public Intelligence disclosed that HBGary, again in partnership with General Dynamics, are developing "a software tool, which provides the user a command line interface, that will enable single file, or full directory exfiltration over TCP/IP."

Called "Task Z," General Dynamics "requested multiple protocols to be scoped as viable options, and this quote contains options for VoIP (Skype) protocol, BitTorrent protocol, video over HTTP (port 80), and HTTPS (port 443)."

As I reported last year, the Obama administration will soon be seeking legislation that would force telecommunications companies to redesign their system and information networks to more readily facilitate internet spying.

And, as the administration builds upon and quietly expands previous government programs that monitor the private communications of the American people, *The New York Times* revealed that our "change" regime will demand that software and communication providers build backdoors accessible to law enforcement and intelligence agencies.

Such "backdoors" will enable spooks trolling "encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype" the means "to intercept and unscramble encrypted messages."

These are precisely the technological "fixes" which firms like HBGary, General Dynamics and presumably other defense contractors are actively building for their secret state security partners.

The Fire This Time

While denouncing China, Russia and other capitalist rivals over cyber espionage and alleged hacking escapades, the deployment of digital weapons of mass destruction against selected adversaries, Iran for one, is an essential feature of Pentagon targeting profiles and has now been fully integrated into overall U.S. strategic military doctrine.

This is hardly the stuff of wild speculation considering that evidence suggests that last year's attack on Iran's civilian nuclear program via the highly-destructive Stuxnet worm was in all probability a joint U.S.-Israeli operation as *The New York Times* disclosed.

Nor should we forget, that U.S. Cyber Command (USCYBERCOM), the Pentagon satrapy directed by NSA Director, Gen. Keith Alexander, is "a sub-unified command subordinate to U. S. Strategic Command," the lead agency charged with running space operations, information warfare, missile defense, global command, control, intelligence, surveillance and reconnaissance (C4ISR), global strike and strategic deterrence; the trigger finger on America's first-strike nuclear arsenal.

Will the next crisis trigger an onslaught against an adversary's civilian infrastructure? *The Washington Post* informs us that an unnamed U.S. official acknowledged that "'the United States is actively developing and implementing' cyber-capabilities 'to deter or deny a potential adversary the ability to use its computer systems' to attack the United States."

However, while the "collateral effects" of such an attack are claimed to be "unpredictable," one can be sure that civilian populations on the receiving end of a Pentagon cyber attack will suffer mass casualties as water and electrical systems go offline, disease and panic spreads and social infrastructures collapse.

Welcome to America's brave new world of high-tech war crimes coming soon to a theater near you (3D glasses optional).

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, , he is a Contributing Editor with Cyrano's Journal Today. 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.*

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