GlobalResearch
Center for Research on Globalization

Cyber Warfare: Building Attack Tools for Mass Destruction

By Tom Burghardt
Theme: Militarization and WMD
Global Research, May 27, 2009
Antifascist Calling... 27 May 2009

A quintessential hallmark of an authoritarian regime, particularly one that operates within highly-militarized, though nominally democratic states such as ours, is the maintenance of a system of internal control; a seamless panopticon where dissent is equated with criminality and the rule of law derided as a luxury ill-afforded "during a time of war."

In this context, the deployment of new *offensive* technologies which can wreck havoc on human populations deemed expendable by the state, are always couched in a *defensive* rhetoric by militarist aggressors and their apologists.

While the al-Qaeda brand may no longer elicit a compelling response in terms of mobilizing the population for new imperial adventures, novel threats–and panics–are required to marshal public support for the upward transfer of wealth into the corporate trough. Today, "cyber terror" functions as the "new Osama."

And with Congress poised to pass the **Cybersecurity Act of 2009**, an Orwellian bill that would give the president the power to "declare a cybersecurity emergency" and shut down or limit Internet traffic in any "critical" information network "in the interest of national security" of course, the spaces left for the free flow of information–and meaningful dissent–slowly contract.

DARPA–and Cybersecurity Grifters–to the Rescue

But protecting critical infrastructure from hackers, criminals and terrorists isn't the only game in town. The Pentagon is planning to kick-start a new office, **Cyber Command**, armed with the capacity to launch devastating attacks against any nation or group deemed an official enemy by Washington.

As *Antifascist Calling* **reported** last year, the Defense Advanced Research Projects Agency (**DARPA**), the Pentagon's "geek squad," is building a National Cyber Range (NCR). As Cyber Command's research arm, the agency's Strategic Technology Office (**STO**) describes **NCR** 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. Leveraging DARPA's history of cutting-edge research, the NCR will revolutionize the state of the art for large-scale cyber testing. Ultimately, the NCR will provide a revolutionary, safe, fully automated and instrumented environment for our national cyber security research organizations to evaluate

> leap-ahead research, accelerate technology transition, and enable a place for experimentation of iterative and new research directions. ("National Cyber Range," Defense Advanced Research Projects Agency, Strategic Technology Office, no date)

According to a January 2009 **press release**, the agency announced that NCR "will accelerate government research and development in high-risk, high-return areas and work in close cooperation with private-sector partners to jump-start technical cyber transformation."

Given the Pentagon's proclivity to frame debates over defense and security-related issues as one of "dominating the adversary" and discovering vulnerabilities that can be "exploited" by war planners, one can hypothesize that NCR is a testing range for the creation of new offensive weapons.

Amongst the "private-sector partners" chosen by the agency to "develop, field, and test new 'leap ahead' concepts and capabilities" are:

BAE Systems, Information and Electronic Systems Integration Inc., Wayne, N.J. , General Dynamics, Advanced Information Systems, San Antonio, Texas; Johns Hopkins University Applied Physics Laboratory, Laurel Md.; Lockheed Martin Corp., Simulation, Training and Support, Orlando, Fla.; Northrop Grumman, Intelligence, Surveillance and Reconnaissance Systems Division, Columbia, Md.; Science Applications International Corp., San Diego, Calif.; SPARTA, Columbia, Md.

While little-known outside the defense and intelligence establishment, **SPARTA** describes its "core business areas" as "strategic defense and offense systems, tactical weapons systems, space systems." Its security and intelligence brief includes "intelligence production, computer network operations, and information assurance."

Investigative journalist James Bamford wrote in ***The Shadow Factory*** that SPARTA "hired Maureen Baginski, the NSA's powerful signals intelligence director, in October 2006, as president of its National Security Systems Sector." According to Bamford, the firm, like others in the netherworld of corporate spying are always on the prowl for intelligence analysts "to pursue access and exploitation of targets of interest."

Given their spooky resume, information on SPARTA's contracts are hard to come by. Indeed, the firm claims that under Section 508 of the Rehabilitation Act they are exempt from providing the public with information because their products involve "the operation, or use of... intelligence activities... related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or systems which are critical to the direct fulfillment of military or intelligence missions." How's that for openness and transparency! One can only hazard a guess as to the firm's role in devising DARPA's "leap-ahead" National Cyber Range.

While the initial outlay of defense funds for NCR may appear to be a substantial amount of boodle for enterprising contractors, it is merely a down payment on Phase I of the project. Melissa Hathaway, the Obama administration's director of the Joint Interagency Cyber Task Force said, "I don't believe that this is a single-year or even a multi-year investment–it's a multi-decade approach."Â Hathaway, a former consultant at the **spooky** Booz Allen Hamilton corporation, told the Intelligence and National Security Alliance (**INSA**) in April,

> Building toward the architecture of the future requires research and development that focuses on game-changing technologies that could enhance the security, reliability, resilience and trustworthiness of our digital infrastructure. We need to be mindful of how we, government and industry together, can optimize our collective research and development dollars and work together to improve market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services. ("Remarks by Melissa E. Hathaway, Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils," INSA, April 30, 2009)

That Hathaway chose INSA as a forum is hardly surprising. Describing itself as a "non-profit professional association created to improve our nation's security through an alliance of intelligence and national security leaders in the private and public sectors," INSA was created by and for contractors in the heavily-outsourced shadow world of U.S. intelligence. Founded by BAE Systems, Booz Allen Hamilton, Computer Sciences Corporation, General Dynamics, Hewlett-Packard, Lockheed Martin, ManTech International, Microsoft, the Potomac Institute and Science Applications International Corporation, *The Washington Post* **characterized** INSA as "a gathering place for spies and their business associates."

"Partners" who benefit directly from the launch of DARPA's National Cyber Range. No doubt, Hathaway's remarks are music to the ears of "beltway bandits" who reap hundreds of billions annually to fund taxpayer-fueled "national security priorities." That the Pentagon is richly rewarding INSA-connected firms with documented track records of "misconduct such as contract fraud and environmental, ethics, and labor violations," according to the Project on Government Oversight's (**POGO**) Federal Contractor Misconduct Database (**FCMD**) hardly elicits a yawn from Congress.

Among the corporations selected by the agency to construct the National Cyber Range, Lockheed Martin leads the pack in "Misconduct $ since 1995" according to POGO, having been fined $577.2 million (**No. 1**); Northrop Grumman, $790.4 million (**No. 3**); General Dynamics, $63.2 million (**No. 4**); BAE Systems, $1.3 million (**No. 6**); Science Applications International Corporation (SAIC), $14.5 million (**No. 9**); Johns Hopkins University, $4.6 million, (**No. 81**)

But as disturbing as these figures are, representing corporate grifting on a massive scale, equally troubling is the nature of the project itself. As *Aviation Week* **reports**, "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."

High-Tech Tools for Aggressive War

The American defense establishment is devising tools that can wreck havoc with a keystroke. DARPA is currently designing "future attack devices" that can be deployed across the imperialist "battlespace" by the "non-expert," that is by America's army of robosoldiers. According to *Aviation Week*, one such device "combines cybersleuthing, technology analysis and tracking of information flow. It then offers suggestions to the operator on how best to mount an attack and, finally, reports on success of the effort."

> The heart of this attack device is its ability to tap into satellite communications, voice over Internet, proprietary Scada networks–virtually any wireless network. Scada (supervisory control and data acquisition) is of particular interest since it

> is used to automatically control processes at high-value targets for terrorists such as nuclear facilities, power grids, waterworks, chemical plants and pipelines. The cyberattack device would test these supposedly inviolate networks for vulnerabilities to wireless penetration. (David A. Fulghum, "Network Attack Weapons Emerge," Aviation Week, May 21, 2009)

As can be expected, the Pentagon's rhetorical *mise-en-scene* is always a purely "defensive" response to future depredations by nefarious and shadowy forces threatening the *heimat*. In fact, the United States has systematically employed battlefield tactics that target civilian infrastructure as a means of breaking the enemy's will to fight. Stretching across the decades, from Southeast Asia to Iraq to Yugoslavia, imperialist strategists have committed war crimes by targeting the electrical grid, water supply and transportation- and manufacturing infrastructure of their adversaries.

The NCR will potentially serve as a new and improved means to bring America's rivals to their knees. Imagine the capacity for death and destruction implicit in a tool that can, for example, at the push of a button cause an adversary's chemical plant to suddenly release methyl isocynate (the Bhopal effect) on a sleeping city, or a nuclear power plant to go supercritical, releasing tens of billions of curies of radioactive death into the atmosphere?

During NATO's 1999 "liberation" of the narco-state Kosovo from the former Yugoslavia, American warplanes dropped what was described as a graphite "blackout bomb," the BLU-114/B "soft bomb" on Belgrade and other Serbian cities during its war of aggression. As the *World Socialist Web Site* **reported** at the time,

A particularly dangerous consequence of the long-term power blackout is the damage to the water systems in many Yugoslav cities, which are dependent on pumping stations run by electrical power. Novi Sad, a city of 300,000 which is the capital of the Vojvodina province of Serbia, has been without running water for eight days, according to residents. Families have been compelled to get water from the Danube river to wash and operate the toilet, and a handful of wells to provide drinking water.

> Sewage treatment plants have also been shut down, with the result that raw, untreated sewage has begun to flow into the network of rivers that feed into the Danube, central Europe's most important waterway. (Marty McLaughlin, "Wall Street celebrates stepped-up bombing of Serbia," World Socialist Web Site, May 5, 1999)

With technological advances courtesy of DARPA's National Cyber Range and their "private-sector partners," the potential for utterly devastating societies ripe for resource extraction by American corporatist war criminals will increase exponentially. As *Wired* **reported**,

> Comparisons between nuclear and cyberweapons might seem strained, but there's at least one commonality. Scholars exploring the ethics of wielding logic bombs, Trojan horses, worms and bots in wartime often find themselves treading on ground tilled by an earlier generation of Cold War nuclear gamesmen.
>
> "There are lots of unknowns with a cyberattack," says Neil Rowe, a professor at the Center for Information Security Research at the U.S. Naval Postgraduate School, who rejects cyberattacks as a legitimate tool of war. "The potential for collateral damage is worse than nuclear technology.... With cyber, it can

> spread through the civilian infrastructure and affect far more civilians." (Marty Graham, "Welcome to Cyberwar Country, USA," Wired, February 11, 2008)

Initiatives such as the National Cyber Range are fully theorized as one facet of "network-centric warfare," the Rumsfeldian "Revolution in Military Affairs." Durham University geographer Stephen Graham **describes** the Pentagon notion that dominance can be achieved through "increasingly omnipotent surveillance and 'situational awareness', devastating and precisely-targeted aerial firepower, and the suppression and degradation of the communications and fighting ability of any opposing forces."

Indeed, these are integrated approaches that draw from corporate management theory to create "continuous, always-on support for military operations in urban terrain," an imperialist battlespace where Wal-Mart seamlessly morphs into The Terminator.

According to *Aviation Week*, the device currently being field tested will "capture expert knowledge but keep humans in the loop." As a battlefield weapon, simplicity and ease of operation is the key to successfully deploying this monstrous suite of tools. And Pentagon "experts" are designing a console that will "quantify results so that the operator can put a number against a choice," "enhance execution by creating a tool for the nonexpert that puts material together and keeps track of it" and finally, "create great visuals so missions can be executed more intuitively."

> A touch-screen dashboard beneath the network schematic display looks like the sound mixing console at a recording studio. The left side lists cyberattack mission attributes such as speed, covertness, attribution and collateral damage. Next to each attribute is the image of a sliding lever on a long scale. These can be moved, for example, to increase the speed of attack or decrease collateral damage. (Aviation Week, op. cit.)

A tunable device for increased destructive capabilities; what are these if not a prescription for mass murder on a post-industrial scale?

Additionally, DARPA sorcerers are combining "digital tools that even an inexperienced operator can bring into play. In the unclassified arena there are algorithms dubbed Mad WiFi, Air Crack and Beach. For classified work, industry developers also have a toolbox of proprietary cyberexploitation algorithms."

What has been dubbed "Air Crack" deploys "open source tools to crack the encryption key for a wireless network." Cryptoattacks on the other hand, "use more sophisticated techniques to cut through the password hash."

One means to "penetrate" an adversary's protective cyber locks is referred to as a "de-authorization capability." According to *Aviation Week*, the attack operator "can kick all the nodes off a network temporarily so that the attack system can watch them reconnect. This provides information needed to quickly penetrate the network."Â As *The Register* **reported** in January when the ink on the DARPA contracts had barely dried,

> Thus the planned Cyber Range must be able to simulate not just large computer networks teeming with nodes, but also the people operating and using these interlocked networks. These software sim-people–users, sysadmins, innocent network bystanders and passers-by–are referred to in the

> Range plans as “replicants”. It seems clear that they won’t know that they are merely simulated pawns in a virtual network wargame designed to test the efficiency of America’s new cyber arsenal. They will merely have to live in a terrible **Groundhog Day** electronic armageddon, where the weapons and players change but destruction and suffering remain eternal. (Lewis Page, “Deals inked on DARPA’s Matrix cyber VR,” The Register, January 5, 2009)

Rance Walleston, the head of BAE’s cyber warfare division told ***Aviation Week*** in late 2008, “We want to change cyber attack from an art to a science.” And as *The Register* averred, the Pentagon’s “simulated cyber warzone” should be up and running next year, “ready to pass under the harrow of BAE’s new electronic pestilences, digital megabombs and tailored computer plagues.”

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****.*

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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