GlobalResearch
Center for Research on Globalization

Massive Cuts in Social Spending to Finance the Pentagon's "Cybersecurity" Gravy Train

By Tom Burghardt
Global Research, April 04, 2011
antifascist-calling.blogspot.com 4 April 2011

Region: USA
Theme: Militarization and WMD, Poverty & Social Inequality

Call it another sterling example of corporate-flavored "bipartisanship."

With a government shut-down looming over a manufactured "deficit crisis," the World Socialist Web Site reports that the "Obama administration and congressional Democrats have offered to triple the amount of cuts in social spending for the remainder of the current fiscal year, from $10 billion to $30 billion, in ongoing talks with congressional Republicans that face an April 8 deadline."

Leftist critic Patrick Martin comments that these "cuts would be the largest ever imposed in a single year's federal budget." If passed, the "cumulative effect" of slashing social spending in FY2011 will be "much greater" over time. In fact, according to estimates, "the House Republican plan would result in social spending that is $1 trillion lower over ten years."

Grand Theft Wall Street

While legislators in a score of states are slashing unemployment benefits, medical care and educational opportunities for Americans hit hardest by the crisis, *Zero Hedge* reports that at the beginning of the 2008 financial meltdown the largest U.S. banks "scrambled to the Fed to soak up any and all available liquidity after confidence in the entire ponzi collapsed."

Hardly a shocker considering that investment banking giant Goldman Sachs, as *McClatchy* revealed, "peddled more than $40 billion in securities backed by at least 200,000 risky home mortgages, but never told the buyers it was secretly betting that a sharp drop in U.S. housing prices would send the value of those securities plummeting."

As investigative journalist Greg Gordon reported, "Goldman's clandestine wagers" completed just before the overinflated housing bubble burst like a putrescent boil, "enabled the nation's premier investment bank to pass most of its potential losses to others before a flood of mortgage defaults staggered the U.S. and global economies."

According to *Zero Hedge*, once the system entered full crisis mode, with share prices plummeting and pension funds, insurance firms, labor unions and overseas financial houses facing catastrophic losses and potential collapse, Federal Reserve Bank Chairman Ben Bernanke mandated that the Primary Dealer Credit Facility be "downgraded to accept collateral of any type," and that the very institutions responsible for the crisis "had the temerity to pledge bonds that had defaulted (i.e. had a rating of D)." In fact, *Zero Hedge* revealed, "the Fed would accept Defaulted bonds as collateral: or 'assets' that have no

value whatsoever"!

Within a few weeks "this practice became pervasive, with virtually every banker pledging defaulted bonds in exchange for money good cash with which to pretend these banks were doing just fine (not to mention that $71.7 billion in collapsing equities represented nearly half the total collateral of $164.3 billion pledged to receive $155 billion in cash.)"

And whom, pray tell, with a wink and a nod from Bush, and now Obama administration "deficit hawks" gamed the system best? Why Goldman Sachs and JP Morgan Chase of course!

It gets better. *ProPublica* tells us that while teachers, nurses and other greedy public sector workers (you know, Leona Helmsley's "little people") have their rights stripped away, pay for bank executives "seems to have been immune to the recession and unaffected by the bailouts."

According to a report in *American Banker* cited by the investigative news site, "in 2003, the banking industry's 1.3 million full-time employees took home $78.3 billion. In 2010, its 2.1 million employees took home $168.1 billion."

ProPublica's Marian Wang informs us "that the point here is the trend, not the actual average. The figure mixes the modest wages of bank tellers with the big bonuses for top execs and investment bankers."

"CEOs, of course," notes Wang, "are still pulling in millions." Bank of America for example "made headlines this week for what seemed to be a cut to CEO Brian Moynihan's compensation. But the $1.94 million he's reported to have taken home in 2010 doesn't include the more than $9 million in deferred compensation that he's due to receive this year."

A sweet deal if you can get it, which of course, you can't.

Instead, for misplaced loyalties to a system intent on grinding us underfoot and charging us for the privilege, *The Wall Street Journal* reported that despite an alleged "improvement in the labor market, many workers are barely treading water as their wages fail to keep up with rising prices."

"Compared with a year earlier," the *Journal* avers, "average inflation-adjusted wages have declined."

Unsurprisingly, "the weakness in wages comes amid surging corporate profits and continued productivity gains. With unemployment still high–8.8% in March–employers are finding so much labor available that they are able to keep a tight lid on wages."

These latest outrages come hard on the heels of reports that arms, nuke plant and media giant (can you say Fukashima Daiichi 1-6 *and* NBC), General Electric, will pay no federal income taxes this year despite "earning" some $14.1 billion in 2010 profits. Under Congress' watchful eye, GE stands to rake in a $3.2 billion tax credit for offshoring U.S. jobs to low wage platforms in various managed democracies.

Rather rich considering that our Grifter-in-Chief, hope and change huckster Barack Obama, named GE's CEO Jeffrey Immelt to head the president's Council on Jobs and Economic

Competitiveness back in January, *Bloomberg News* reported.

No surprise here once you learn, as OpenSecrets.org did, that GE doled out some $39.2 million in 2010 lobbying the best Congress money can buy.

The *World Socialist Web Site* avers, with troglodytic Republicans demanding some $61 billion in social spending cuts at the behest of crazed Tea Party groups bankrolled by billionaires, "progressive" Democrats have agreed to meet their henchmen half-way across the aisle, a process called "splitting the difference" that will result in "cuts of approximately $33 billion."

"A bipartisan group of 64 senators, 32 from each party, signed a joint letter to Obama," Martin observes, urging the president "to 'engage' personally in talks on long-term deficit reduction, which would include major cuts in Social Security, Medicare and Medicaid, the three most costly federal social programs."

Want to guess who's demanding more from an ever-dwindling federal pie, largely the result of multiple imperial wars to steal other people's resources, corporate bailouts, tax cuts for the filthy rich and a National Surveillance State that views the American people as their deadliest enemy?

All Aboard the "Cybersecurity" Gravy Train

As *Antifascist Calling* has frequently reported, with various cyber panics now supplementing secret state scaremongering over terrorist threats from a score of shady actors, more often than not off-the-shelf "irregular forces" who, when not murdering official U.S. enemies, i.e., leftists, human rights campaigners, trade unionists and other opponents of Empire, do a brisk business trafficking arms, drugs, human organs, women, whatever.

Orwell reminds us: "All the war-propaganda, all the screaming and lies and hatred, comes invariably from people who are not fighting." But that doesn't mean they can't make a killing when opportunity comes knocking. After all, as *Market Research Media* reported, "with a cumulative market valued at $55 billion (2010-2015), the U.S. Federal Cybersecurity market will grow steadily–at about 6.2% CAGR over the next six years."

Panic sells, and once the terms of the debate have been set by interested parties adept at feathering their nests, well, it's all aboard the "cybersecurity" gravy train!

Last month, *NextGov* disclosed that "protecting military networks" in FY2012 will "cost nearly $1 billion more than the Pentagon publicly reported last month, an increase that reflects the growing number of programs being re-categorized as cybersecurity-related, agency officials said."

When the Obama administration released its 2012 budget back in February, "the Pentagon announced it was requesting $2.3 billion to bolster network security within the Defense Department and to strengthen ties with its counterparts at the Homeland Security Department, which is responsible for overseeing civilian cybersecurity," reporter Aliya Sternstein wrote.

But as I reported last year, "strengthening ties" amongst civilian and military cyber warriors means that the "Memorandum of Agreement" struck between the Department of Homeland

Security and the National Security Agency will inevitably lead to a marked increase of Pentagon control, in profitable alliance with major defense and security firms, over America's telecommunications and electronic infrastructure.

A reflexive power-grab by the Pentagon is not however, a sign that the internet and related telecommunications' platforms are being absorbed by that scarecrow beloved by neoliberals, libertarians and other "free market" fanatics: "big government." As Marxist social media critic Christian Fuchs points out:

Foucault characterized surveillance in the following way: "He is seen, but he does not see; he is the object of information, never a subject in communication." With the rise of "web 2.0," the Internet has become a universal communication system, which is shaped by privileged data control by corporations that own most of the communication-enabling web platforms and by the state that can gain access to personal data by law. … By being subjects of communication on the Internet, users make available personal data to others and continuously communicate over the Internet. These communications are mainly mediated by corporate-owned platforms, therefore the subjects of communication become objects of information for corporations and the state in surveillance processes. … In web 2.0, corporate and state power is exercised through the gathering, combination, and assessment of personal data that users communicate over the web to others, and the global communication of millions within a heteronomous society produces the interest of certain actors to exert control over these communications. In web 2.0, power relations and relationships of communication are interlinked. The users are producers of information … but this creative communicative activity enables the controllers of disciplinary power to closely gain insights into the lives, secrets, and consumption preferences of the users. (Christian Fuchs, "Web 2.0, Prosumption, and Surveillance," *Surveillance & Society*, Vol. 8, No. 3, p. 304)

In this light, the Pentagon's obsessive secrecy, particularly as it relates to "cybersecurity" and programs designed for offensive cyber war, its management-driven cult of controlling informational flows and pathological aversion to democratic decision-making processes are anything *but* antithetical to a neoliberal regime that commodifies everything and values nothing. Rather, the broader militarization of society and social relations as a whole, characterized by endless imperial wars and a system of generalized plunder must be viewed as an expression, albeit a sinister one, of capitalism's drive to privatize and commodify the state itself as a profit-generating center.

This is clearly the case when it comes to Defense Department inflation of their FY2012 cybersecurity budgets. While it is certainly true that the military is the "consumer" of cyber-related "products," it is the *producers* of those products, defense and security corporations who drive market demand. As investigative journalist Tim Shorrock uncovered in his landmark study, *Spies For Hire*, "the bulk of this $50 billion [intelligence] market is serviced by one hundred companies, ranging in size from multibillion-dollar defense behemoths to small technology shops funded by venture capitalists that have yet to turn a profit."

In a follow-up piece, *NextGov* revealed while "the White House proposed spending $2.3 billion on cybersecurity at the Defense Department … simultaneously Air Force officials announced their cybersecurity request would be $4.6 billion."

For their part, the "Army and Defense Information Systems Agency referred inquiries about their proposed cyber spending to department-level officials." And "Navy officials said they

could not provide a top-line budget figure, since funding that supports Navy cybersecurity activities is scattered across several line items, as well as multiple programs, organizations and commands."

As Sternstein points out, while "the area surrounding 'cybersecurity' funding is gray … the various interpretations of cybersecurity spending translate into real-world financial and national security costs, budget and technology."

Defense Department spokeswoman April Cunningham told *NextGov*, that the Air Force "included things that we, [at the department's office of the chief information officer] categorize as IT infrastructure, or other activities–not directly information assurance."

"According to the department," Sternstein writes, "information assurance consists of five programs, including public key infrastructure, or digital certificates, as well as defense industrial base cybersecurity for private sector assets that support the military."

Cunningham said that "activities at the Air Force and other services that Defense considers to be 'information assurance-cybersecurity' are captured in the total $3.2 billion figure." And "based on this formula" the Army is seeking $432 million and the Navy are lusting after $347 million in FY2012.

However, other Defense agencies "including DISA, the National Security Agency and the Defense Advanced Research Projects Agency–are asking for a cumulative $1.6 billion. Details on proposed cyber spending at all Pentagon components are shared with Congress in a classified budget book, she said."

Which means, given the Pentagon's propensity to quietly hide their most controversial programs within the dark folds of the black budget, Congress, let alone the American people, really have no idea what such programs entail, who benefits from black contract outlays and ultimately, how they'll be deployed.

NextGov reported that the revised budget request "also includes funding for noninformation assurance activities" that the Pentagon claims "are integral to the military's cyber posture, specifically cyber operations, security innovations and forensics."

Additionally, "the budget assigns $159 million to the relatively new U.S. Cyber Command, and distributes $258 million among science and technology investments targeted at cyber tools," and that "some" of the proposed funding will go "toward a new partnership with the Homeland Security Department, which oversees civilian cyber operations."

“Any way you measure it,” Sternstein writes, “Defense funding for cybersecurity dwarfs that of Homeland Security. The fiscal 2012 budget for DHS information security is $936 million.”

And given the fact that “some cybersecurity funding is classified at Defense components such as the NSA,” the Pentagon satrapy with the brief to driftnet spy on Americans’ communications and potentially, through U.S. Cyber Command, carry out offensive operations against selected domestic targets in tandem with corporate partners, as the HBGary emails and documents leaked by Anonymous seem to suggest, total cybersecurity spending is an immense black hole.

As investigative journalist Nate Anderson revealed in *Ars Technica*, the HBGary hack demonstrated how the U.S. government is now “in the position of deploying the hacker’s darkest tools–rootkits, computer viruses, trojan horses, and the like.”

Indeed, Anderson reports, in 2009 “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 was focused on delivering such tools in tandem with defense giant General Dynamics “which a later e-mail makes clear was for a government agency.”

“Hoglund’s special interest was in all-but-undetectable computer ‘rootkits’,” *Ars Technica* reported, “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.”

According to a 243 page report by HBGary, “Windows Rootkit Analysis Report,” posted by the secrecy-shredding web site *Public Intelligence*, Hoglund averred that “combining deployment of a rootkit with a BOT makes for a very stealth piece of malicious software.”

A companion document published by *Public Intelligence*, “Proposal for Project C,” informs us that “General Dynamics has selected HBGary Inc to provide this proposal for development of a software application targeting the Windows XP Operating System that, when executed, loads and enables a covert kernel-mode implant that will exfiltrate a file from disk (or other remotely called commands) over a connected serial port to a remote device.”

We’re informed that the “enabling kernel mode implant will cater to a command and control element via the serial port,” which “as part of the exploit delivery package, a usermode trojan will assist in the loading of the implant, which will clearly demonstrate the full capability of the implant.”

In plain English: private contractors, including some of the largest U.S. defense and security firms, are busy as proverbial bees designing malware for the secret state; insidious, undetectable applications that can transform an individual’s laptop or smart phone into a component of a malicious botnet under cover of “cyber defense.”

Try finding those line items in the Defense Department’s FY2012 budget!

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.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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