The Secret State's Mad Scheme to Control the Internet

by Tom Burghardt via Kismo - Antifascist Calling *Sunday, Jun 27 2010, 9:13pm*
international / mass media / other press

> Prussian military theorist Carl von Clausewitz once famously wrote that "war is the continuation of politics by other means." A century later, radical French philosopher Michel Foucault turned Clausewitz on his head and declared that "politics is the continuation of war by other means." In our topsy-turvy world where truth and lies coexist equally and sociopathic business elites reign supreme, it would hardly be a stretch to theorize that cyber war is the continuation of parapolitical crime by other means.

Through the Wormhole

In *Speed and Politics*, cultural theorist Paul Virilio argued that "history progresses at the speed of its weapons systems." With electronic communications now blanketing the globe, it was only a matter of time before our political masters, (temporarily) outflanked by the subversive uses to which new media lend themselves, would deploy what Virilio called the "integral accident" (9/11 being one of many examples) and gin-up entirely new categories of threats, "Cyber Pearl Harbor" comes to mind, from which of course, they would "save us."

That the revolving door connecting the military and the corporations who service war making is a highly-profitable redoubt for those involved, has been analyzed here at great length. With new moves to tighten the screws on the immediate horizon, and as "Change" reveals itself for what it always was, an Orwellian exercise in public diplomacy, hitting the "kill switch" serves as an apt descriptor for the new, repressive growth sector that links technophilic fantasies of "net-centric" warfare to the burgeoning "homeland security" market.

Back in March, *Wired* investigative journalist Ryan Singel wrote that the "biggest threat to the open internet" isn't "Chinese hackers" or "greedy ISPs" but corporatist warriors like former Director of National Intelligence Mike McConnell.

Having retreated to his old haunt as a senior vice president with the ultra-spooky firm Booz Allen Hamilton (a post he held for a decade before joining the Bush administration), McConnell stands to make millions as Booz Allen's parent company, the secretive private equity powerhouse, The Carlyle Group, plans to take the firm public and sell some $300 million worth of shares, *The Wall Street Journal* reported last week.

"With its deep ties to the defense establishment" the *Journal* notes, "Booz Allen has become embedded in a range of military operations such as planning war games and intelligence initiatives." That Carlyle Group investors have made out like proverbial bandits during the endless "War on Terror" goes without saying. With "relatively low debt levels for a leveraged buyout," the investment "has been a successful one for Carlyle, which has benefited from the U.S. government's increasing reliance on outsourcing in defense."

And with 15,000 employees in the Washington area, most with coveted top secret and above security

clearances, Booz Allen's clients include a panoply of secret state agencies such as the CIA, the Defense Intelligence Agency, the Department of Homeland Security, NSA and the U.S. Air Force. With tentacles enlacing virtually all facets of the secretive world of outsourced intelligence, the firm has emerged as one of the major players in the cybersecurity niche market.

While McConnell and his minions may not know much about "SQL injection hacks," Singel points out that what makes this spook's spook dangerous (after all, he was NSA Director under Clinton) "is that he knows about social engineering. ... And now he says we need to re-engineer the internet."

Accordingly, *Washington Technology* reported in April, that under McConnell's watchful eye, the firm landed a $14.4 million contract to build a new bunker for U.S. Cyber Command (CYBERCOM). Chump change by Pentagon standards perhaps, but the spigot is open and salad days are surely ahead.

Now that CYBERCOM has come on-line as a "subordinate unified command" of U.S. Strategic Command (STRATCOM), it's dual-hatted Director, Air Force General Keith B. Alexander confirmed by the Senate and with a fourth, gleaming star firmly affixed on his epaulettes, the *real* fun can begin.

A denizen of the shadows with a résumé to match, Alexander is also Director of the National Security Agency (hence the appellation "dual-hatted"), the Pentagon satrapy responsible for everything from battlefield signals- and electronic intelligence (SIGINT and ELINT), commercial and industrial espionage (ECHELON) to illegal driftnet spying programs targeting U.S. citizens.

Spooky résumé aside, what should concern us here is what Alexander will actually *do* at the Pentagon's new cyberwar shop.

A Fact Sheet posted by STRATCOM informs us that CYBERCOM "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."

As *Antifascist Calling* previously reported, CYBERCOM's offensive nature is underlined by the role it will play as STRATCOM's operational cyber wing. The training of thousands of qualified airmen, as *The Register* revealed last month, will form the nucleus of an "elite corps of cyberwarfare operatives," underscoring the command's signal importance to the secret state and the corporations they so lovingly serve.

Cybersecurity: The New Corporatist "Sweet Spot"

Fueling administration moves to "beef up," i.e. tighten state controls over the free flow of information is cash, lots of it. *The Washington Post* reported June 22 that "Cybersecurity, fast becoming Washington's growth industry of choice, appears to be in line for a multibillion-dollar injection of federal research dollars, according to a senior intelligence official."

"Delivering the keynote address at a recent cybersecurity summit sponsored by Defense Daily," veteran *Post* reporter and CIA media asset, Walter Pincus, informs us that "Dawn Meyerriecks, deputy director of national intelligence for acquisition and technology, said that along with the White House Office of Science and Technology, her office is going to sponsor major research 'where the government's about to spend multiple billions of dollars'."

Bingo!

According to a *Defense Daily* profile, before her appointment by Obama's recently fired Director of National Intelligence, Dennis C. Blair, Meyerriecks was the chief technology officer with the Defense Information Systems Agency (DISA), described on DISA's web site as a "combat support agency" that "engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations."

During *Defense Daily's* June 11 confab at the Marriott Hotel in Washington (generously sponsored by Northrop Grumman, Raytheon, General Dynamics and The Analysis Group), Meyerriecks emphasized although "tons of products" have been commercially developed promising enhanced security, "there's not an answer Band-Aid that is going to come with this."

All the more reason then, to shower billions of taxpayer dollars on impoverished defense and security corps, while preaching "fiscal austerity" to "greedy" workers and homeowners facing a new wave of foreclosures at the hands of cash strapped banks.

"We're starting to question whether or not the fundamental precepts are right," Meyerriecks said, "and that's really what, at least initially, this [new research] will be aimed at."

Presumably, the billions about to feed the "new security paradigm," all in the interest of "keeping us safe" of course, means "we need to be really innovative, because I think we're going to run out of runway on our current approach," she said.

Washington Technology reported Meyerriecks as saying "We don't have any fixed ideas about what the answers are." Therefore, "we're looking for traditional and nontraditional partnering in sourcing."

Amongst the "innovative research" fields which the ODNI, the Department of Homeland Security and one can assume, NSA/CYBERCOM, will soon be exploring are what *Washington Technology* describe as: "Multiple security levels for government and non-government organizations. Security systems that change constantly to create 'moving targets' for hackers," and more ominously for privacy rights, coercive "methods to motivate individuals to improve their cybersecurity practices."

The Secret State's Internet Control Bill

Since major policy moves by administration flacks always come in waves, Homeland Security Secretary Janet Napolitano told the American Constitution Society for Law and Policy June 18, that in order to fight "homegrown terrorism" the monitoring of internet communications "is a civil liberties trade-off the U.S. government must make to beef up national security," the *Associated Press* reported.

While the Obama regime has stepped-up attacks on policy critics who have disclosed vital information concealed from the American people, prosecuting whistleblowers such as Thomas Drake, who spilled the beans on corrupt NSA shenanigans with grifting defense and security corps, and wages a low-level war against *WikiLeaks*, Cryptome, *Public Intelligence* and other secret spilling web sites, it continues to shield those who oversaw high crimes and misdemeanors during the previous and *current* regimes.

In this light, Napolitano's statement that "we can significantly advance security without having a deleterious impact on individual rights in most instances," is a rank mendacity.

With enough airspace to fly a drone through, the Home Sec boss told the gathering "at the same time, there are situations where trade-offs are inevitable." What those "situations" are or what "trade-offs" were being contemplated by the administration was not specified by Napolitano; arch neocon Joe Lieberman however, graciously obliged.

As "Cyber War" joins the (failed) "War on Drugs" and the equally murderous "War on Terror" as America's latest *bête noire* and panic all rolled into one reeking mass of disinformation, Senators Joseph Lieberman (ID-CT), Susan Collins (R-ME) and Tom Carper (D-DE) introduced the Protecting Cyberspace as a National Asset Act of 2010 in the Senate.

The bill empowers the Director of a new National Center for Cybersecurity and Communications (NCCC), to be housed in the Department of Homeland Security, to develop a "process" whereby owners and operators of "critical infrastructure" will develop "response plans" for what the legislation calls "a national cybersecurity emergency."

This particularly pernicious piece of legislative flotsam would hand the President the power to declare a "national cyber-emergency" at his discretion and would force private companies, internet service providers and search engines to "comply with the new risk-based security requirements." Accordingly, "in coordination with the private sector ... the President [can] authorize emergency measures to protect the nation's most critical infrastructure if a cyber vulnerability is being exploited or is about to be exploited."

Under terms of the bill, such "emergency measures" can force ISPs to "take action" if so directed by the President, to limit, or even to sever their connections to the internet for up to 30 days.

While the administration, so far, has not explicitly endorsed Lieberman's bill, DHS Deputy Undersecretary Philip Reitinger told reporters that he "agreed" with the thrust of the legislation and that the Executive Branch "may need to take extraordinary measures" in the event of a "crisis."

Under the 1934 Communications Act, the *World Socialist Web Site* points out, "the president may, under 'threat of war,' seize control of any 'facilities or stations for wire communications'."

"Though dated," socialist critic Mike Ingram avers, "that definition would clearly apply to broadband providers or Web sites. Anyone disobeying a presidential order can be imprisoned for one year. In addition to making explicit the inclusion of Internet providers, a central component of the Lieberman bill is a promise of immunity from financial claims for any private company which carries through an order from the federal government."

Under terms of the legislation, the president requires no advance notification to Congress in order to hit the internet "kill switch," and his authority to reign supreme over the free speech rights of Americans can be extended for up to six months after the "state of war" has expired.

While the bill's supporters, which include the secret state lobby shop, the Intelligence and National Security Alliance (INSA) claim the Lieberman-Collins-Carper legislation is intended to create a "shield" to defend the U.S. and its largest corporate benefactors from the "looming threat" of a "Cyber 9/11," one cannot discount the billions of dollars in plum government contracts that will fall into the laps of the largest defense and security corps, the primary beneficiaries of this legislation; thus the bill's immunity provisions.

Indeed, current INSA Chairwoman, Frances Fragos Townsend, the former Bushist Homeland Security Adviser, was appointed in 2007 as National Continuity Coordinator under the auspices of National Security Presidential Directive 51 (NSPD-51) and was assigned responsibility for coordinating the development and implementation of Federal continuity of government (COG) policies. As readers of *Antifascist Calling* are aware, plans include contingencies for a declaration of martial law in the event of a "catastrophic emergency." Whether or not a "national cybersecurity emergency" would fall under the penumbral cone of silence envisaged by NSPD-51 to "maintain order" is anyone's guess.

However, in a June 23 letter to Lieberman-Collins-Carper, the Center for Democracy and Technology (CDT) and 23 other privacy and civil liberties groups, insisted that "changes are needed to ensure that cybersecurity measures do not unnecessarily infringe on free speech, privacy, and other civil liberties interests."

CDT states that while "the bill makes it clear that it does not authorize electronic surveillance beyond that authorized in current law, we are concerned that the emergency actions that could be compelled could include shutting down or limiting Internet communications that might be carried over covered critical infrastructure systems."

Additionally, CDT avers that the bill "requires CCI owners to share cybersecurity 'incident' information with DHS, which will share some of that information with law enforcement and intelligence personnel." While Lieberman-Collins-Carper claim that "incident reporting" doesn't authorize "any federal entity" to compel disclosure "or conduct surveillance," the bill does not indicate what might be included in an 'incident report' and we are concerned that personally-identifiable information will be included." Count on it!

In a press release, INSA's chairwoman declared that the legislation is important in "establishing a public-private partnership to promote national cyber security priorities, strengthen and clarify authorities regarding the protection of federal civilian systems, and improve national cyber security defenses."

Amongst the heavy-hitters who will profit financially from developing a "public-private partnership to promote national cyber security priorities," include INSA "Founding Members" BAE Systems, Booz Allen Hamilton, CSC, General Dynamics, HP, Lockheed Martin, ManTech International, Microsoft, Potomac Institute for Policy Studies and Science Applications International Corporation (SAIC).

Talk about one hand washing the other! A casual glance at *Washington Technology's* 2010 list of the Top 100 Federal Government Contractors provides a telling definition of the term "stakeholder"!

Blanket Surveillance Made Easy: Einstein 3's Roll-Out

During a recent Cyberspace Symposium staged by the Armed Forces Communications and Electronics Association (AFCEA), an industry lobby group chock-a-block with defense and security corps, a series of video presentations set the tone, and the agenda, for CYBERCOM and the secret state's new push for *heimat* cybersecurity.

During a question and answer session "with a small group of reporters" in sync with the alarmist twaddle peddled by AFCEA and STRATCOM, *Defense Systems'* Amber Corrin informed us that "one possibility" floated by Deputy Defense Secretary William Lynne III to "keep us safe," is the deployment of the privacy-killing Einstein 2 and Einstein 3 intrusion detection and prevention

systems on civilian networks.

"To support such a move" *Defense Systems* reported, "a task force comprising industry and government information technology and defense interests ... has been forged to examine issues surrounding critical infrastructure network security."

As *Antifascist Calling* reported last July, Einstein 3 is based on technology developed by NSA under its Tutelage program, a subordinate project of NSA's larger and more pervasive privacy-killing Stellar Wind surveillance operation.

Einstein 3's deep-packet inspection technology can read the content of email messages and other private electronic communications. Those deemed "threats" to national security networks can then be forwarded to analysts and "attack signatures" (or suspect political messages) are then stored in a massive NSA-controlled database for future reference.

Federal Computer Week disclosed in March that the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) "plans to partner with a commercial Internet Service Provider and another government agency to pilot technology developed by the National Security Agency to automate the process of detecting cyber intrusions into civilian agencies' systems."

"The exercise," according to reporter Ben Bain "aims to demonstrate the ability of an ISP to select and redirect Internet traffic from a participating government agency using the new technology. The exercise would also be used demonstrate the ability for U.S. CERT to apply intrusion detection and prevention to that traffic and to generate automated alerts about selected cyber threats."

That testing is currently underway and has been undertaken under authority of National Security Presidential Directive 54, signed by President George W. Bush in 2008 in the waning days of his administration. While the vast majority of NSPD-54 is classified top secret, hints of its privacy-killing capabilities were revealed in the sanitized version of the Comprehensive National Cybersecurity Initiative (CNCI) released by the Obama White House in March.

The Electronic Privacy Information Center (EPIC) has filed suit against the government in federal court after their Freedom of Information Act request to the National Security Agency was rejected by securocrats. The agency refused to release NSPD-54, since incorporated into Obama's CNCI, stating that they "have been withheld in their entirety" because they are "exempt from release" on grounds of "national security."

In a follow-up piece earlier this month, *Federal Computer Week* disclosed that the exercise "will also allow the Homeland Security Department, which runs the Einstein program, to share monitored information with the National Security Agency, though that data is not supposed to include message content."

"The recent combination of those three elements--reading e-mail messages, asking companies to participate in the monitoring program, and getting the NSA in the loop--has set off alarm bells about future uses of Einstein 3," *FCW's* John Zyskowski disclosed.

Those bells have been ringing for *decades*, tolling the death of our democratic republic. As military-style command and control systems proliferate, supporting everything from "zero-tolerance" policing and urban surveillance, the deployment of packet-sniffing technologies will soon join CCTV cameras, license plate readers and "watchlists," thus setting the stage for the next phase of the secret state's

securitization of daily life.

http://antifascist-calling.blogspot.com/2010/06/through-wormhole-secret-states-mad.html

---