GlobalResearch
Center for Research on Globalization

Obama's Cybersecurity Plan

Bring in the Contractors!

By Tom Burghardt
Global Research, June 04, 2009
Antifascist Calling 4 June 2009

Region: USA
Theme: Police State & Civil Rights

With billions of dollars in federal funds hanging in the balance, President Barack Obama unveiled the Cyberspace Policy Review May 29 at the White House.

During his presentation in the East Room Obama said that "America's economic prosperity in the 21st century will depend on cybersecurity" and that efforts to "deter, prevent, detect and defend" against malicious cyberattacks would be run from the White House.

How this debate is being framed however, has a familiar ring to it. Rather than actually educating the public about steps to prevent victimization, state prescriptions always seem to draw from the same tired playbook.

First, issue dire warnings of an imminent national catastrophe; second, manufacture a panic with lurid tales of a "digital Pearl Harbor;" third, gin-up expensive "solutions" that benefit armies of (well-paid) experts drawn from officialdom and the private sector (who generally are as interchangeable as light bulbs however dim).

As Wired magazine's "Threat Level" editor Kevin Poulsen said during a panel at the Computers, Freedom and Privacy conference in Washington June 3, "the threat of cyber-terrorism is 'preposterous'," arguing that "long-standing warnings" that hackers will attack the nation's power grid is so much hot-air. Poulsen contends "that calling such intrusions national security threats means information about attacks gets classified unneccessarily."

While the president claims the new office "will not include–I repeat will not include–monitoring private sector networks or Internet traffic," and that his administration "will preserve and protect the personal privacy and civil liberties that we cherish as Americans," the devil is in the details and when they're added together "change" once again, morphs into more of the same.

As with all things Washington, lurking wraith-like in the background, amidst bromides about "protecting America" from "cyber thieves trolling for sensitive information" are the usual class of insiders: the well-heeled corporations and their stable of retired militarists and spies who comprise the Military-Industrial-Security Complex.

Take Dale Meyerrose, for example. The former Air Force Major General served as U.S. Northern Command's Chief Information Officer. After a stint at NORTHCOM, Meyerrose became Deputy Director of National Intelligence for Information Sharing for U.S. Director of National Intelligence Mike McConnell, the former NSA Director and ten-year executive vice president at the spooky Booz Allen Hamilton firm.

Last week, Meyerrose told The Wall Street Journal that "one important challenge will be finding a way to persuade private companies, especially those in price-sensitive industries, to invest more money in digital security. 'You have to figure out what motivates folks,' he said."

He should know. After serving as McConnell's cyber point man, Meyerrose plotted a new flight plan that landed him a plum job with major defense contractor, the Harris Corporation, where he currently directs the company's National Cyber Initiative.

Headquartered in Melbourne, Florida, the firm boasts $5.4 billion in annual revenue and clocked in at No. 13 on Washington Technology's "2008 Top 100 Government Contractors" list, with some $1.6 billion in defense-related income. Under the General Services Administration's Alliant contract worth some $50 billion, the firm is competeing with other defense giants to provide an array of IT services to various federal agencies. Major customers include the Federal Aviation Administration, the National Reconnaissance Office and Defense Department.

Let's be clear: "What motivates folks" is cold, hard cash and there's lots of it to go around courtesy of the American people. The New York Times reported May 31, "The government's urgent push into cyberwarfare has set off a rush among the biggest military companies for billions of dollars in new defense contracts." According to the Times,

> The exotic nature of the work, coupled with the deep recession, is enabling the companies to attract top young talent that once would have gone to Silicon Valley. And the race to develop weapons that defend against, or initiate, computer attacks has given rise to thousands of "hacker soldiers" within the Pentagon who can blend the new capabilities into the nation's war planning.
>
> Nearly all of the largest military companies–including Northrop Grumman, General Dynamics, Lockheed Martin and Raytheon–have major cyber contracts with the military and intelligence agencies. (Christopher Drew and John Markoff, "Contractors Vie for Plum Work, Hacking for the United States," The New York Times, May 31, 2009)

As Washington Technology reported June 1, Zal Azmi, CACI International's senior vice president for strategic law enforcement and national security programs, told the insider publication: "The timing is perfect. There is a lot of enthusiasm for it. "It's a very comprehensive plan. It lays out a very good strategy."

And there you have it.

A Cybersecurity Dream: Bundles of Cash

Although the position of Cybersecurity Coordinator has yet to be filled, its a sure bet whoever gets the nod will be drawn from a narrow pool of security executives, the majority of whom transit effortlessly between the Pentagon and defense corporations. That individual will oversee billions of dollars in funding for developing and coordinating the defense of computer systems that operate the global financial system as well as domestic transportation and commerce.

Under the administration's plan, the Cybersecurity Coordinator will report to the president's National Economic Council (NEC) and the National Security Council (NSC). The CSC will be a

member of both NEC and NSC, Obama said in his East Room statement, "an acknowledgment that the threat is both to national security and to the economy," The Washington Post reports.

According to the Post, Obama's top economic adviser, Lawrence H. Summers, fought for a dominant role for the NEC, ensuring that "efforts to protect private networks do not unduly threaten economic growth." This however, is unlikely to happen given the make-up of the administration's team. Which raises the question: who exactly were Obama's "private sector partners" who helped devise current state policy? The Cyberspace Policy Review sets the record straight.

> The U.S. depends upon a privately owned, globally operated digital infrastructure. The review team engaged with industry to continue building the foundation of a trusted partnership. This engagement underscored the importance of developing value propositions that are understood by both government and industry partners. It also made clear that increasing information sharing is not enough; the government must foster an environment for collaboration. The following industry groups and venues participated: the Armed Forces Communications and Electronics Association (AFCEA), Business Executives for National Security (BENS), the Business Software Alliance (BSA), the Center for Strategic and International Studies' (CSIS) Commission on Cybersecurity for the 44th Presidency, the Communications Sector Coordinating Council (C-SCC), the Cross-Sector Cyber Security Working Group (CSCSWG), the Defense Industrial Base Executive Committee, the Financial and Banking Information Infrastructure Committee (FBIIC), the Financial Services Sector Coordinating Council (FS-SCC), the Intelligence and National Security Alliance (INSA), the Internet Security Alliance (ISA), the Information Technology Sector Coordinating Council (IT-SCC), the National Infrastructure Advisory Council (NIAC), the National Security Telecommunications Advisory Committee (NSTAC), TechAmerica, and the U.S. Chamber of Commerce. (Cyberspace Policy Review, Appendix B: Methodology, pp. B 2-3.)

A bevy of heavy-hitters in the defense, banking, financial services, intelligence and security industries if ever there were one. And much like their predecessors in the Oval Office, the Obama administration has failed to "guard against the acquisition of unwarranted influence" by the Military-Industrial-Security Complex which president Dwight. D. Eisenhower so eloquently warned against–and expanded–decades ago.

Round Up the Usual Suspects

Who then are the new peddlers of "unwarranted influence"? Let's take a look.

Armed Forces Communications and Electronics Association (AFCEA): The Fairfax, Virginia group describes itself as a "non-profit membership association serving the military, government, industry, and academia" to advance "professional knowledge and relationships in the fields of communications, IT, intelligence and global security." AFCEA was founded at the dawn of the Cold War in 1946. It serves as an "ethical forum" where "a close cooperative relationship among government agencies, the military and industry" is fostered. With 32,000 individual and 1,700 corporate members, AFCEA was described by investigative journalist Tim Shorrock in his essential book Spies For Hire as "the largest industry association in the intelligence business." Its board of directors and executive committee are studded with players drawn from major defense and security firms such as CACI

International, Booz Allen Hamilton, Science Applications International Corporation, ManTech International Corporation, QinetiQ North America, General Dynamics, Lockheed Martin and the spooky MITRE Corporation.

Business Executives for National Security (BENS): This self-described "nationwide, non-partisan organization" claims the mantle of functioning as "the primary channel through which senior business executives can help advance the nation's security." BENS members were leading proponents of former vice president Al Gore's defense reform initiative that handed tens of billions of taxpayer dollars to BENS members in the heavily-outsourced intelligence and security industries. An advocacy group with a distinct neoconservative tilt, BENS "one special interest: to help make America safe and secure" is facilitated by executives drawn from the Pentagon. Its current Chairman and CEO is retired Air Force General Charles G. Boyd who served as former House Speaker Newt Gingrich's "defense consultant." Its board of directors and executive committee include members from Biltmore Capital Group, LLC; Janus Capital Group, Booz Allen Hamilton, Cisco Systems Inc., Perot Systems Inc., Goldman Sachs and The Tupperware Corporation (!) to name but a few. BENS Advisory Council includes major war criminal Henry Kissinger, former Treasury Secretary Robert Rubin, former U.N. Ambassador Thomas Pickering, former FBI and CIA Director William Webster, former CIA head honcho Michael V. Hayden and former Chairman of the Joint Chiefs of Staff, General Peter Pace. "Non-partisan" indeed!

Business Software Alliance (BSA): BSA describes itself as "the largest and most international IT industry group" comprised on the "most innovative companies in the world." Its members are drawn from the top corporations in the computing and software industries and include Adobe, Apple, Cisco Systems, Dell, Hewlett-Packard, IBM, Intel, Microsoft, Siemens and Symantec. Most of these firms have extensive contractual arrangements with the Defense Department.

Center for Strategic and International Studies (CSIS): For decades, CSIS has been a major right-wing think tank closely tied to the defense and security industries. Since its founding in 1962 by David Abshire and Admiral Arleigh Burke, CSIS has been a mouthpiece for the Defense and Intelligence Complex. Its current President and CEO, John J. Hamre was a former Deputy Secretary of Defense in the Clinton administration and was hired by SAIC to work on the National Security Agency's scandal-plagued Trailblazer program. The $361 million project to build a new communications intercept system for NSA was described as a "colossal failure" by investigative journalists Donald Bartlett and James Steele in a 2007 piece in Vanity Fair. CSIS was a major behind-the-scenes force urging the 2003 U.S. invasion and occupation of Iraq and was an apologist for the Bush administration's bogus allegation that the Iraqi government possessed "weapons of mass destruction," citing "poor intelligence" rather than political mendacity on a grand scale. In the aftermath of the invasion, Booz Allen Hamilton organized a "major conference on rebuilding Iraq that attracted hundreds of corporations eager to cash in on the billions of dollars in contracts about to be awarded by the Bush administration," according to Tim Shorrock. The closed-door event was held in the CSIS conference room and outlined the Bush regime's plans for Iraq's economic make-over–one that would sell-off state assets "in a way very conducive to foreign investment." The Obama administration's Cyberspace Policy Review has drawn extensively from CSIS' Securing Cyberspace for the 44th Presidency report, an alarmist screed that avers that "cybersecurity is now a major national security problem for the United States." Indeed the CSIS report urges the Obama administration to "reinvent the public-private partnership" with "a focus on operational activities" that "will result in more

progress on cybersecurity." How might this be accomplished? Why by regulating cyberspace, of course! CSIS avers that "voluntary action is not enough," and states "we advocate a new approach to regulation that avoids both prescriptive mandates, which could add unnecessary costs and stifle innovation, and overreliance on market forces, which are ill-equipped to meet national security and public safety requirements." But with a dubious track record dating back to the Cold War, and a board of directors manned by multinational defense grifters and neoconservative/neoliberal insiders such as former U.S. Senator Sam Nunn, Henry Kissinger, Richard Armitage, Zbigniew Brzezinski, former Defense Secretary William S. Cohen, James R. Schlesinger and Bush crime family insider Brent Scowcroft, CSIS' cybersecurity prescriptions are anything but reliable.

Communications Sector Coordinating Council (CSCC): Created in 2005 "to represent the Communications Sector, as the principal entity for coordinating with the government in implementing the National Infrastructure Protection Plan (NIPP)," CSCC's "unique industry-government partnership" facilitates the "exchange of information among government and industry participants regarding vulnerabilities, threats, intrusions and anomalies affecting the telecommunications infrastructure." Certainly one "anomaly" not addressed by CSCC is the National Security Agency's driftnet surveillance of Americans' private communications. A major hub where telecommunications' grifters meet, CSCC members include AT&T, Boeing, Cisco Systems, Comcast, Computer Sciences Corporation, Level 3, the MITRE Corporation, Motorola, the National Association of Broadcasters, Nortel, Quest, Sprint, Tyco, U.S. Internet Service Provider Association, VeriSign and Verizon. Many of the above-named entities are direct collaborators with the NSA and FBI's extensive warrantless wiretapping programs.

Intelligence and National Security Alliance (INSA): As Antifascist Calling reported May 26, INSA was created by and for contractors in the heavily-outsourced 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." According to an INSA paper on cybersecurity, Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment, the group recommended "a single leadership position at the White House-level that aligns national cyber security responsibilities with appropriate authorities." Among other prescriptions, reflecting the group's close ties to defense firms and the Pentagon INSA calls on the Obama administration to "establish a stronger working relationship between the private sector and the U.S. Government" (!) With their members heavily-banking on an expansion of Pentagon development of cyber attack tools, the group calls on the state to "Incorporate private sector cyber threat scenarios within government cyber-related test beds (e.g., DARPA's Cyber Test Range). Government cyber-related test beds should reflect private sector operational scenarios, especially to demonstrate how similar threats are detected and deterred, as well as to demonstrate private sector concerns (e.g., exploitation of electric utility control system)." As I previously reported, INSA founding members BAE Systems, General Dynamics, Lockheed Martin and SAIC have all been awarded contracts by DARPA to build and run the National Cyber Range.

Internet Security Alliance (ISA): According to a self-promotional blurb on their website, ISA "was created to provide a forum for information sharing" and "represents corporate security interests before legislators and regulators." Amongst ISA sponsors one finds AIG (yes, that AIG!) Verizon, Raytheon, VeriSign, the National Association of Manufacturers, Nortel,

Northrop Grumman, Tata, and Mellon. State partners include the U.S. Department of Homeland Security, Congress, and the Department of Commerce. Among ISA's recommendations for the Obama administration's Cyberspace Policy Review was its unabashed claim that "the diversity of the internet places its security inescapably in the hands of the private sector." When one considers that the development of the Internet was the result of taxpayer dollars, ISA's cheeky demand is impertinent at best, reflecting capitalism's inherent tendency to "forget" who foots the bill! In this vein, ISA believes that "government's first role ought to be to use market incentives to motivate adhering to good security practices." In other words, taxpayer-financed handouts. Considering the largess already extended to ISA "sponsor" AIG, "regulation for consumer protection" that use "government mandates" to "address cyber infrastructure issues" will be "ineffective and counter-productive both from a national security and economic perspective." Give us the money seems to be ISA's clarion call to the new "change" regime in Washington. And why not? Just ask AIG!

The Information Technology Sector Coordinating Council (IT-SCC): According to their website, the IT-SCC was established in 2006 and brought together "companies, associations, and other key IT sector participants," in a forum that "envisions a secure, resilient and protected global information infrastructure that can rapidly restore services if affected by an emergency or crisis," and may "consider the use of government resources to support appropriate tasks such as administrative, meeting logistics, specifically defined and mutually agreeable projects, and communications support (particularly in response to government requests or needs)." With some six dozen corporate members, the majority of whom are heavily-leveraged in the defense and security industries, IT-SCC affiliates include the usual suspects: Business Software Alliance, Center for Internet Security, Computer Sciences Corporation, General Dynamics, IBM, Intel, Internet Security Alliance, ITT Corporation, Lockheed Martin, Microsoft, Northrop Grumman, Perot Systems, Raytheon and Verizon, to name but a few. One IT-SCC affiliate not likely craving public scrutiny is Electronic Warfare Associates, Inc. (EWA). According to Wired, one EWA company, the Herndon, Virginia-based EWA Government Systems, Inc., "is one of several firms that boasts of making tiny devices to help manhunters locate their prey. The company's 'Bigfoot Remote Tagging System' is a "very small, battery-operated device used to emit an RF [radio frequency] transmission [so] that the target can be located and/or tracked." Allegedly in use along the AfPak border, the devices are RFID beacons planted by local operatives "near militant safehouses," which guide CIA Predator and Reaper drones to their targets. Sounds like any number of government-sponsored "mutually agreeable projects" to me!

The National Security Telecommunications Advisory Committee (NSTAC): As Antifascist Calling reported last year (see: "Comcast's Spooky Employment Opportunities") NSTAC is comprised of telecom executives representing the major communications, network service providers, information technology, finance and aerospace companies who provide "industry-based advice and expertise" to the President "on issues and problems relating to implementing national security and emergency preparedness communications policy," according to SourceWatch. Created in 1982 when former president Ronald Reagan signed Executive Order 12382, in all probability NSTAC facilitates U.S. telecommunication firms' "cooperation" with NSA and other intelligence agencies' efforts in conducting warrantless wiretapping, data-mining and other illegal surveillance programs in highly-profitable arrangements with the Bush and Obama administrations. NSTAC's current Chair is Edward A. Mueller, Chairman and CEO at Qwest. The group's Vice Chair is John T. Stankey, the President and CEO at AT&T. Additional corporate members include: The Boeing Company,

Motorola, Science Applications International Corporation, Lockheed Martin, Rockwell International, Juniper Networks, the Harris Corporation, Tyco Electronics, Computer Sciences Corporation, Microsoft, Bank of America, Inc., Verizon, Raytheon and Nortel.

TechAmerica: Self-described as "the driving force behind productivity growth and jobs creation in the United States," TechAmerica represents some 1,500 member companies and "is the industry's largest advocacy organization," one that "is dedicated to helping members' top and bottom lines." Indeed, the lobby shop offered lavish praise for president Obama's Cyber Security plan. Calling the administration's Cyberspace Policy Review a "historic step in the right direction," one that will "protect America" (wait!) "from a digital 9/11."

Conclusion

The Obama administration's Cyberspace Policy Review is a corporatist boondoggle that will neither ameliorate nor frankly, even begin to address the most pertinent cybersecurity threats faced by the vast majority of Americans: hacking and spoofing attacks by criminals. Why? The wretched programs riddled with bad code and near non-existent "security" patches breeched as soon as they're written are not part of the playbook. Indeed, the corporations and software developers who've grown rich off of the Internet have no incentive to write better programs!

After all, from a business perspective its far better to terrorize the public into demanding more intrusive, and less accountable, minders who will "police" the Internet–for a hefty price.

Posted by Antifascist at 2:49 PM

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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