GlobalResearch
Center for Research on Globalization

Tracking People Online: The "Cyberwar" Against The American People is Over. The National Security Agency Has Won

By Tom Burghardt
Global Research, October 20, 2010
Antifascist Calling... 20 October 2010

Region: USA
Theme: Police State & Civil Rights

A "**Memorandum of Agreement**" struck last week between the Department of Homeland Security (DHS) and the National Security Agency (NSA) promises to increase Pentagon control over America's telecommunications and electronic infrastructure.

It's all in the interest of "cybersecurity" of course, or so we've been told, since much of the Comprehensive National Cybersecurity Initiative (CNCI) driving administration policy is a closely-held state secret.

Authority granted the über spy shop by the Bush and Obama administrations was handed to NSA by the still-classified National Security Presidential Directive 54, Homeland Security Presidential Directive 23 (NSPD 54/HSPD 23) in 2008 by then-President Bush.

The Agreement follows closely on the heels of reports last week by the Electronic Frontier Foundation (**EFF**) that DHS has been tracking people online and that the agency even established a "Social Networking Monitoring Center" to do so.

Documents obtained by EFF through a Freedom of Information Act **lawsuit**, revealed that the agency has been vacuuming-up "items of interest," systematically monitoring "citizenship petitioners" and analyzing "online public communication."

The **documents** suggest that "DHS collected a massive amount of data on individuals and organizations explicitly tied to a political event," the Obama inauguration.

This inevitably raises a troubling question: what other "political events" are being monitored by government snoops? Following last month's raids on antiwar activists by heavily-armed FBI SWAT teams, the answer is painfully obvious.

And with new reports, such as Monday's revelations by ***The Wall Street Journal*** that Facebook "apps" have been "transmitting identifying information–in effect, providing access to people's names and, in some cases, their friends' names–to dozens of advertising and Internet tracking companies," online privacy, if such a beast ever existed, is certainly now a thing of the past.

Project 12

With waning national interest in the "terrorism" product line, the "cybersecurity" roll-out (in stores in time for the holidays!) will drive hefty taxpayer investments–and boost the share

price–for America's largest defense and security firms; always a sure winner where it counts: on Wall Street.

The DHS-NSA Agreement came just days after publication of a leaked document obtained by the secrecy-shredding web site Public Intelligence (**PI**).

> "In early 2008," a PI analyst **writes**, "President Bush signed National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) formalizing the Comprehensive National Cybersecurity Initiative (CNCI). This initiative created a series of classified programs with a total budget of approximately $30 billion. Many of these programs remain secret and their activities are largely unknown to the public."

Amongst the programs stood up by CNCI "is an effort to encourage information sharing between the public and private sector called 'Project 12'."

The whistleblowing web site "recently acquired the key **report** from the Project 12 meetings: *Improving Protection of Privately Owned Critical Network Infrastructure Through Public-Private Partnerships*. This 35-page, For Official Use Only report is a guide to creating public-private partnerships that facilitate the implementation of 'actionable recommendations that [reflect] the reality of shared responsibility between the public and private sectors with respect to securing the nation's cyber assets, networks, systems, and functions'."

According to the document, under the rubric of the National Infrastructure Protection Plan (NIPP), Project 12 recommends that "critical infrastructure and key resources (CIKR) be brought into federal cybersecurity efforts through a variety of means."

As *Antifascist Calling* readers are well aware, for decades the secret state has outsourced "inherently governmental" functions to private entities. This process has served as a means to both shield illegal activities and avoid public accountability under a cloak of "proprietary business information."

PI's secret spillers tell us that Project 12 stresses the "promotion of public-private partnerships that legalize and facilitate the flow of information between federal entities and private sector critical infrastructure, such as telecommunications and transportation."

> "The ultimate goal of these partnerships" the analyst writes, "is not simply to increase the flow of 'threat information' from government agencies to private industry, but to facilitate greater 'information sharing' between those companies and the federal government."

What information is to be shared or what the implications are for civil liberties and privacy rights are not spelled out in the report.

As can readily be seen in the dubious relationships forged amongst retired senior military personnel and the defense industry, a top level Pentagon position is entrée to an exclusive club where salary levels and perks, increase the higher one has climbed the food chain.

Much the same can be said for high-level intelligence officials. Indeed, former officials turned corporate executives constellating the security industry are among the most

vociferous advocates for strengthening collaboration between the state and private sectors. And the more powerful players on the field are represented by lobby shops such as the Intelligence and National Security Alliance (**INSA**) and Business Executives for National Security (**BENS**).

Last year I **reported** that BENS are key players driving the national "cybersecurity" panic. In that piece I wrote that the group is a "self-described 'nationwide, non-partisan organization' [that] claims the mantle of functioning as 'the primary channel through which senior business executives can help advance the nation's security'." Project 12 is one area where BENS power-brokers have excelled in mutual backscratching.

We are informed that "the cost of scoping and building a tool that meets the requirements for cyber real-time situational awareness is likely to be significant and would be a high-risk investment of Federal funding." In other words, while taxpayers foot the bill, private corporations will reap the benefits of long-term contracts and future high-tech development projects.

However, "before making that investment, the U.S. Government and its information sharing security partners must define a clear scope and mission for the development of common situational awareness and should evaluate a variety of interim or simplified solutions."

Those "solutions" won't come cheap.

Market Research Media informs us that "the U.S. government sector witnesses a blossoming of investments in cyber security technologies."

We're told that with a "cumulative market valued at $55 billion (2010-2015), the U.S. Federal Cybersecurity market will grow steadily–at about 6.2% CAGR [compound annual growth rate] over the next six years."

Those numbers reflect the merger and acquisition mania amongst America's largest defense and security firms who are gobbling up the competition at ever-accelerating rates.

Washington Technology reported earlier this month that "government contractors specializing in the most attractive niche segments of the market are experiencing much more rapid growth and, accordingly, enjoying much higher valuation multiples upon selling their businesses than their more generalist counterparts."

> "The larger companies in the federal market" the insider publication reports, "continue to seek to aggressively position themselves as leaders in the cyber market."

Amongst the "solutions" floated by Project 12 is the notion that "real-time" awareness can be achieved when "government resources" are "co-located with private industry, either virtually or physically, to help monitor security," the PI's analyst avers.

Therefore, "physical or virtual co-location would maximize the U.S. Government's investment in network protection by facilitating collaborative analysis and coordinated protective and response measures and by creating a feedback loop to increase value for private-sector and government participants. Another key outcome would be stronger

institutional and personal trust relationships among security practitioners across multiple communities."

One firm, the spooky Science Applications International Corporation (SAIC) "formally opened its seven-story cyber innovation center in Columbia, not far from the site of the new Cyber Command at Fort Meade," NSA headquarters, ***The Washington Post*** reported.

Talk about "co-location"! It doesn't get much chummier than this!

In order to valorize secret state investments in the private sector, the development of "Information Sharing and Analysis Centers (ISACs)," or fusion centers, are encouraged. Who would control the information flows and threat assessments are unknown.

However, as the American Civil Liberties Union documented in their report, ***What's Wrong with Fusion Centers***, private sector participation in the intelligence process "break[s] down the arm's length relationship that protects the privacy of innocent Americans who are employees or customers of these companies" while "increasing the risk of a data breach."

This is all the more troubling when the "public-private partnership" envisioned by Project 12 operate under classified annexes of the Comprehensive National Cybersecurity Initiative.

NSA "Power-Grab"

Last year Rod Beckström, director of Homeland Security's National Cybersecurity Center (NCSC), resigned from his post, citing threats of a NSA "power grab."

In a **letter** highly-critical of government efforts to "secure" the nation's critical infrastructure, Beckström said that NSA "effectively controls DHS cyber efforts through detailees [and] technology insertions."

Citing NSA's role as the secret state's eyes and ears peering into electronic and telecommunications' networks, Beckström warned that handing more power to the agency could significantly threaten "our democratic processes…if all top level government network security and monitoring are handled by any one organization."

The administration claimed last week that the Agreement will "increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities," and that DHS and NSA will embed personnel in each agency.

We're informed that the Agreement's implementation "will focus national cybersecurity efforts, increasing the overall capacity and capability of both DHS's homeland security and DoD's national security missions, while providing integral protection for privacy, civil rights, and civil liberties."

Accordingly, the "Agreement is authorized under the provisions of the Homeland Security Act (2002); the Economy Act; U.S. Code Title 10; Executive Order 12333; National Security Directive 42; Homeland Security Presidential Directive-5; Homeland Security Presidential Directive-7; and National Security Presidential Directive 54/Homeland Security Presidential Directive-23."

What these "authorizations" imply for civil liberties and privacy rights are not stated. Indeed, like NSPD 54/HSPD 23, portions of **National Security Directive 42**, **HSPD 5**, and **HSPD 7** are also classified.

And, as described above, top secret annexes of NSPD 54/HSPD 23 enabling the Comprehensive National Cybersecurity Initiative means that the American people have no way of knowing what these programs entail, who decides what is considered "actionable intelligence," or where–and for what purpose–private communications land after becoming part of the "critical infrastructure and key resources" landscape.

We're told that the purpose of the Agreement "is to set forth terms by which DHS and DoD will provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities."

The text specifies that the Agreement will "focus national cybersecurity efforts" and provide "integral protection for privacy, civil rights, and civil liberties."

However, as the premier U.S. eavesdropping organization whose "national security mission" is responsible for setting data encryption standards, NSA was ultimately successful in weakening those standards in the interest of facilitating domestic spying.

Indeed, ***The Wall Street Journal*** reported in 2008 "the spy agency now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records."

Investigative journalist Siobhan Gorman informed us that the "NSA enterprise involves a cluster of powerful intelligence-gathering programs" that include "a Federal Bureau of Investigation program to track telecommunications data once known as Carnivore, now called the Digital Collection System, and a U.S. arrangement with the world's main international banking clearinghouse to track money movements."

"The effort" the *Journal* revealed, "also ties into data from an ad-hoc collection of so-called 'black programs' whose existence is undisclosed," and include programs that have "been given greater reach" since the 9/11 provocation.

The civilian DHS Cybersecurity Coordinator will take a backseat to the Pentagon since the office "will be located at the National Security Agency (NSA)" and "will also act as the DHS Senior Cybersecurity Representative to U.S. Cyber Command (USCYBERCOM)."

Personnel will be assigned by DHS "to work at NSA as part of a Joint Coordination Element (JCE) performing the functions of joint operational planning, coordination, synchronization, requirement translation, and other DHS mission support for homeland security for cybersecurity," and will "have current security clearances (TS/SCI) upon assignment to NSA, including training on the appropriate handling and dissemination of classified and sensitive information in accordance with DoD, Intelligence Community and NSA regulations."

TS/SCI (Top Secret/Sensitive Compartmented Information) clearances mean that while civilian DHS employees may have access to NSA and Pentagon "black" surveillance programs, they will be restricted from reporting up their chain of command, or to congressional investigators, once they have been "read" into them. This makes a mockery

of assertions that the Agreement does “not alter … command relationships.” The mere fact that DHS personnel will have TS/SCI clearances mean just the opposite.

DHS will “provide appropriate access, administrative support, and space for an NSA Cryptologic Services Group (CSO) and a USCYBERCOM Cyber Support Element (CSE) collocated with the National Cybersecurity and Communications Integration Center (NCCIC), at DHS, and integration into DHS’s cybersecurity operational activities.”

In other words, the civilian, though sprawling DHS bureaucracy will play host for NSA and CYBERCOM personnel answering to the Pentagon, and subject to little or no oversight from congressional committees already asleep at the switch, “to permit both CSG and CSE entities the capability to carry out their respective roles and responsibilities.”

Despite boilerplate that “integral protection for privacy, civil rights, and civil liberties” will be guaranteed by the Agreement, there is no hiding the fact that a NSA power-grab has been successfully executed.

The Agreement further specifies that DHS and NSA will engage “in joint operational planning and mission coordination” and that DHS, DoD, NSA and CYBERCOM “maintain cognizance” of “cybersecurity activities, to assist in deconfliction and promote synchronization of those activities.”

Following Project 12 revelations, new secret state relationships will assist “in coordinating DoD and DHS efforts to improve cybersecurity threat information sharing between the public and private sectors to aid in preventing, detecting, mitigating, and/or recovering from the effects of an attack, interference, compromise, or incapacitation related to homeland security and national security activities in cyberspace.”

However, we do not learn whether “information sharing” includes public access, or even knowledge of, TS/SCI “black programs” which already aim powerful NSA assets at the American people. In fact, the Agreement seems to work against such disclosures.

This is hardly a level playing field since NSA might “receive and coordinate DHS information requests,” NSA controls the information flows “as appropriate and consistent with applicable law and NSA mission requirements and authorities, in operational planning and mission coordination.” The same strictures apply when it comes to information sharing by U.S. Cyber Command.

As Rod Beckström pointed out in his resignation letter, NSA “effectively controls DHS cyber efforts through detailees [and] technology insertions.”

Despite the Agreement’s garbled bureaucratese, we can be sure of one thing: the drift towards militarizing control over Americans’ private communications will continue.

*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**, **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/