Big Brother is Watching You: Pervasive Surveillance Under Obama

The DHS-NSA-AT&T "Cybersecurity" Partnership

By Tom Burghardt

Global Research, October 26, 2013
Antifascist Calling... and Global Research 6 July 2009

Region: USA
Theme: Intelligence, Police State & Civil Rights

Path-breaking article first published on GR in July 2009

Under the rubric of cybersecurity, the Obama administration is moving forward with a Bush regime program to screen state computer traffic on private-sector networks, including those connecting people to the Internet, The Washington Post revealed July 3.

That project, code-named "Einstein," may very well be related to the much-larger, ongoing and highly illegal National Security Agency (NSA) communications intercept program known as "Stellar Wind," disclosed in 2005 by The New York Times.

There are several components to Stellar Wind, one of which is a massive data-mining project run by the agency. As USA Today revealed in 2006, the "National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth."

Under the current program, Einstein will be tied directly into giant NSA data bases that contain the trace signatures left behind by cyberattacks; these immense electronic warehouses will be be fed by information streamed to the agency by the nation's telecommunications providers.

AT&T, in partnership with the Department of Homeland Security (DHS) and the NSA will spearhead the aggressive new initiative to detect malicious attacks launched against government web sites–by continuing to monitor the electronic communications of Americans.

This contradicts President Obama's pledge announcing his administration's cybersecurity program on May 29. During White House remarks Obama said that the government will not continue Bush-era surveillance practices or include "monitoring private sector networks or Internet traffic."

Called the "flagship system" in the national security state's cyber defense arsenal, The Wall Street Journal reports that Einstein is "designed to protect the U.S. government's computer networks from cyberspies." In addition to cost overruns and mismanagement by outsourced contractors, the system "is being stymied by technical limitations and privacy concerns." According to the Journal, Einstein is being developed in three stages:

> Einstein 1: Monitors Internet traffic flowing in and out of federal civilian networks. Detects abnormalities that might be cyber attacks. Is unable to block attacks.
>
> Einstein 2: In addition to looking for abnormalities, detects viruses and other indicators of attacks based on signatures of known incidents, and alerts analysts immediately. Also can't block attacks.
>
> Einstein 3: Under development. Based on technology developed for a National Security Agency program called Tutelage, it detects and deflects security breaches. Its filtering technology can read the content of email and other communications. (Siobhan Gorman, "Troubles Plague Cyberspy Defense," The Wall Street Journal, July 3, 2009)

As readers of Antifascist Calling are well aware, like other telecom grifters, AT&T is a private-sector partner of NSA and continues to be a key player in the agency's driftnet spying on Americans' electronic communications. In 2006, AT&T whistleblower Mark Klein revealed in a sworn affidavit, that the firm's Internet traffic that runs through fiber-optic cables at the company's Folsom Street facility in San Francisco was routinely provided to the National Security Agency.

Using a device known as a splitter, a complete copy of Internet traffic that AT&T receives–email, web browsing requests and other electronic communications sent by AT&T customers, was diverted onto a separate fiber-optic cable connected to the company's SG-3 room, controlled by the agency. Only personnel with NSA clearances–either working for, or on behalf of the agency–have access to this room.

Klein and other critics of the program, including investigative journalist James Bamford who reported in his book, The Shadow Factory, believe that some 15-30 identical NSA-controlled rooms exist at AT&T facilities scattered across the country.

Einstein: You Don't Have to Be a Genius to Know They're Lying

But what happens next, after the data is processed and catalogued by the agency is little understood. Programs such as Einstein will provide NSA with the ability to read and decipher the content of email messages, any and all messages in real-time.

While DHS claims that "the new program will scrutinize only data going to or from government systems," the Post reports that a debate has been sparked within the agency over "uncertainty about whether private data can be shielded from unauthorized scrutiny, how much of a role NSA should play and whether the agency's involvement in warrantless wiretapping during George W. Bush's presidency would draw controversy."

A "Privacy Impact Assessment (PIA) for EINSTEIN 2″ issued by DHS in May 2008, claims the system is interested in "malicious activity" and not personally identifiable information flowing into federal networks.

While DHS claims that "the risk associated with the use of this computer network security intrusion detection system is actually lower than the risk generated by using a commercially available intrusion detection system," this assertion is undercut when the agency states, "Internet users have no expectation of privacy in the to/from address of their messages or the IP addresses of the sites they visit."

When Einstein 3 is eventually rolled-out, Internet users similarly will "have no expectation of privacy" when it comes to the content of their communications.

DHS Secretary Janet Napolitano told reporters, "we absolutely intend to use the technical resources, the substantial ones, that NSA has." Seeking to deflect criticism from civil libertarians, Napolitano claims "they will be guided, led and in a sense directed by the people we have at the Department of Homeland Security."

Despite protests to the contrary by securocrats, like other Bush and Obama "cybersecurity" initiatives the Einstein program is a backdoor for pervasive state surveillance. Government Computer News reported in December 2008 that Marc Rotenberg, the executive director of the Electronic Privacy Information Center (EPIC) said that "the misuse or exposure of sensitive data from such a program [Einstein] could undermine the security arguments for surveillance."

And with Internet Service Providers routinely deploying deep packet inspection tools to "siphon off requested traffic for law enforcement," tools with the ability to "inspect and shape every single packet–in real time–for nearly a million simultaneous connections" as Ars Technica reported, to assume that ISPs will protect Americans' privacy rights from out-of-control state agencies is a foolhardy supposition at best.

The latest version of the system will not be rolled-out for at least 18 months. But like the Stellar Wind driftnet surveillance program, communications intercepted by Einstein 3 will be routed through a "monitoring box" controlled by NSA and their civilian contractors.

> Under a classified pilot program approved during the Bush administration, NSA data and hardware would be used to protect the networks of some civilian government agencies. Part of an initiative known as Einstein 3, the plan called for telecommunications companies to route the Internet traffic of civilian agencies through a monitoring box that would search for and block computer codes designed to penetrate or otherwise compromise networks. (Ellen Nakashima, "Cybersecurity Plan to Involve NSA, Telecoms," The Washington Post, July 3, 2009)

However, investigative journalist Wayne Madsen reported last September "that the Bush administration has authorized massive surveillance of the Internet using as cover a cyber-security multi-billion dollar project called the 'Einstein' program."

While some researchers (including this one) question Madsen's overreliance on anonymous sources and undisclosed documents, in fairness it should be pointed out that nine months before The New York Times described the NSA's secret e-mail collection database known as Pinwale, Madsen had already identified and broken the story. According to Madsen,

> The classified technology being used for Einstein was developed for the NSA in conducting signals intelligence (SIGINT) operations on email networks in Russia. Code-named PINWHEEL, the NSA email surveillance system targets Russian government, military, diplomatic, and commercial email traffic and burrows into the text portions of the email to search for particular words and phrases of interest to NSA eavesdroppers. According to NSA documents obtained by WMR, there is an NSA system code-named "PINWALE."
>
> The DNI and NSA also plan to move Einstein into the private sector by claiming

> the nation’s critical infrastructure, by nature, overlaps into the commercial sector. There are classified plans, already budgeted in so-called “black” projects, to extend Einstein surveillance into the dot (.) com, dot (.) edu, dot (.) int, and dot (.) org, as well as other Internet domains. Homeland Security Secretary Michael Chertoff has budgeted $5.4 billion for Einstein in his department’s FY2009 information technology budget. However, this amount does not take into account the “black” budgets for Einstein proliferation throughout the U.S. telecommunications network contained in the budgets for NSA and DNI. (Wayne Madsen, “‘Einstein’ replaces ‘Big Brother’ in Internet Surveillance,” Online Journal, September 19, 2008)

A follow-up article published in February, identified the ultra-spooky Booz Allen Hamilton firm as the developer of Pinwale, an illegal program for the interception of text communications. According to Madsen, “the system is linked to a number of meta-databases that contain e-mail, faxes, and text messages of hundreds of millions of people around the world and in the United States.”

In other words both classified programs, Pinwale and Einstein, are sophisticated electronic communications surveillance projects that most certainly will train the agency’s formidable intelligence assets on the American people “using as cover a cyber-security multi-billion dollar project called the ‘Einstein’ program,” as Madsen reported.

AT&T: “No Comment”

An AT&T spokesman refused to comment on the proposals and is seeking legal protection from the state that it will not be sued for privacy breaches as a result of its participation in the new program. “Legal certification” the Post reports, “has been held up for several months as DHS prepares a contract.”

NSA’s involvement is critical proponents claim, because the agency has a readily-accessible database of computer codes, or signatures “that have been linked to cyberattacks or known adversaries. The NSA has compiled the cache by, for example, electronically observing hackers trying to gain access to U.S. military systems,” the Post averred.

Calling NSA’s cache “the secret sauce…it’s the stuff they have that the private sector doesn’t,” is what raises alarms for privacy and civil liberties’ advocates. Known as Tutelage, NSA’s classified program can detect and automatically decide how to deal with malicious intrusions, “to block them or watch them closely to better assess the threat,” according to the Post. “The database for the program would also contain feeds from commercial firms and DHS’s U.S. Computer Emergency Readiness Team, administration officials said.”

Jeff Mohan, AT&T’s executive director for Einstein, was more forthcoming earlier this year. He told Federal News Radio: “With these services, we will provide a secure portal from the agency’s infrastructure, or Intranet to the public internet. There is a technical aspect, which is routers, firewalls and that sort of thing that applies these security capabilities across that portal and looks a Internet traffic that comes from public Internet to Intranet and vice versa.”

The “technical aspect” will also provide federal agencies the ability to capture, sort, read and then store Americans’ private communications in huge data bases run by NSA.

Mohan said that AT&T will provide the state with “optional services such as scanning e-mail and placing filters on agency networks to keep malicious e-mail off the network as well as forensic and storage capabilities also are available through MTIPS [Managed Trusted Internet Protocol Services].”

In addition to AT&T, other private partners awarded contracts under the General Services Administration’s MTIPS which has a built-in “Einstein enclave” include: Sprint, L3 Communications, Qwest, MCI, General Dynamics and Verizon, according to multiple reports published by Federal Computer Week.

Claiming that the state is “looking for malicious content, not a love note to someone with a dot-gov e-mail address,” a former unnamed “senior Bush administration official” told the Post “what we’re interested in is finding the code, the thing that will do the network harm, not reading the e-mail itself.”

Try selling that to the tens of millions of Americans whose private communications have been illegally spied upon by the Bush and Obama administrations or leftist dissidents singled-out for “special handling” by the national security state’s public-private surveillance partnership!

An Electronic Spider’s Web

As the “global war on terror” morphs into an endless war on our democratic rights, the NSA is expanding domestic operations by “decentralizing its massive computer hubs,” The Salt Lake Tribune revealed.

The agency “will build a 1-million-square-foot data center at Utah’s Camp Williams,” the newspaper disclosed July 1. The new facility would be NSA’s third major data center. In 2007, the agency announced plans to build a second data center in San Antonio, Texas after the Baltimore Sun reported that NSA had “maxed out” the electric capacity of the Baltimore area’s power grid.

The San Antonio Current reported in December, that the NSA’s Texas Cryptology Center will cost “upwards of $130 million.” The 470,000 square-foot-facility is adjacent to a similar center constructed by software giant Microsoft. Investigative journalist James Bamford told the Current that under current law “NSA could gain access to Microsoft’s stored data without even a warrant, but merely a fiber-optic cable.”

A follow-up article by The Salt Lake Tribune reported that the facility will cost upwards of $2 billion dollars and that funds have already been appropriated by the Obama administration for NSA’s new data center and listening post.

> The secretive agency released a statement Thursday acknowledging the selection of Camp Williams as a site for the new center and describing it as “a specialized facility that houses computer systems and supporting equipment.”
>
> Budget documents provide a more detailed picture of the facility and its mission. The supercomputers in the center will be part of the NSA’s signal intelligence program, which seeks to “gain a decisive information advantage for the nation and our allies under all circumstances” according to the documents. (Matthew D. LaPlante, “New NSA Center Unveiled in Budget Documents,” The Salt Lake Tribune, July 2, 2009)

Not everyone is pleased with the announcement. Steve Erickson, the director of the antiwar Citizens Education Project told the Tribune, “Finally, the Patriot Act has a home.”

While the total cost of rolling-out the Einstein 3 system is classified, The Wall Street Journal reports that “the price tag was expected to exceed $2 billion.” And as with other national security state initiatives, it is the American people who are footing the bill for the destruction of our democratic rights.

The original source of this article is Antifascist Calling... and Global Research

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca