GlobalResearch
Center for Research on Globalization

New Spy Software Coming On-Line: "Surveillance in a Box" Makes its Debut

By Tom Burghardt

Global Research, August 28, 2008
Antifascist Calling... 28 August 2008

Theme: Police State & Civil Rights

You've heard of the FBI's "**Quantico Circuit**" and were outraged by illegal warrantless wiretapping by Bushist minions. To no avail, you flooded Congress with emails and phone calls, angered by the bipartisan "FISA Amendments Act of 2008" and the **swell party** thrown by AT&T for "Blue Dog" Democrats in Denver this week for the convention.

But just in time for a new administration (and the bundles of cash always at the ready for the expanding homeland security market), comes a complete "surveillance in a box" system called the Intelligence Platform!

According to ***New Scientist***, German electronics giant Siemens has developed software allegedly capable of integrating

> ...tasks typically done by separate surveillance teams or machines, pooling data from sources such as telephone calls, email and internet activity, bank transactions and insurance records. It then sorts through this mountain of information using software that Siemens dubs "intelligence modules". (Laura Margottini, "Surveillance Made Easy," New Scientist, 23 August 2008)

New Scientist reports that the firm has sold the system to some 60 countries in Europe and Asia. Which countries? Well, Siemens won't say.

However, privacy and human rights advocates say the system bears a remarkable resemblance to China's "Golden Shield," a massive surveillance network that integrates huge information databases, internet and email monitoring, speech and facial recognition platforms in combination with CCTV monitoring.

Designed specifically for "fusion centers" or their European/Asian equivalents, the Intelligence Platform promises to provide "real-time" high-tech tools to foil terrorist plots before they're hatched (or keep tabs on antiwar/antiglobalization activists).

The latest item in the emerging "intelligent" software niche market, Intelligence Platform has been "trained" on a large number of sample documents to zero in on names, phone numbers or places from generic text. "This means it can spot names or numbers that crop up alongside anyone already of interest to the authorities, and then catalogue any documents that contain such associates," *New Scientist* avers.

In the UK, the Home Office announced it plans to provide law enforcement, local councils

and other public agencies access to the details of text messages, emails and internet browsing. This follows close on the heels of an announcement last May that New Labour was considering building a massive centralized database "as a tool to help the security services tackle crime and terrorism." According to ***The Guardian***,

> Local councils, health authorities and hundreds of other public bodies are to be given the power to access details of everyone's personal text, emails and internet use under Home Office proposals published yesterday.
>
> Ministers want to make it mandatory for telephone and internet companies to keep details of all personal internet traffic for at least 12 months so it can be accessed for investigations into crime or other threats to public safety. …
>
> Conservatives and Liberal Democrats last night branded the measure a "snooper's charter". (Alan Travis, "'Snooper's charter' to check texts and email," The Guardian, Wednesday, August 13, 2008)

A blurb posted on Siemens' **website** claims that the "challenge" is "to foster the well-being of law-abiding citizens" and therefore, "authorized groups need to have direct access to communications between suspects, whether it is individuals, groups or organizations. Only then can they take appropriate action, detect, prevent and anticipate crimes and guarantee peace and security."

In other words, if you've got nothing to hide "trust us:" the shopworn mantra of securocrats everywhere. And in today's climate, this is an especially burdensome challenge for state security and corporate spies who demand "highly-sophisticated, multi-level voice and data recordings" in order to destroy our rights while transforming our respective societies into Orwellian police states. *New Scientist* reports,

> Once a person is being monitored, pattern-recognition software first identifies their typical behaviour, such as repeated calls to certain numbers over a period of a few months. The software can then identify any deviations from the norm and flag up unusual activities, such as transactions with a foreign bank, or contact with someone who is also under surveillance, so that analysts can take a closer look.

But if the experience of U.S. Fusion Centers are any indication of the accuracy of the Siemens system, false positives will be endemic while thousands, if not millions, of perfectly innocent individuals are forever ensnared in the state's data driftnet. According to the **American Civil Liberties Union**,

> The Justice Department's 2006 Guidelines envision fusion centers doing more than simply sharing legitimately acquired law enforcement information across different branches of our burgeoning security establishment. The Guidelines encourage compiling data "from nontraditional sources, such as public safety entities and private sector organizations" and fusing it with federal intelligence "to anticipate, identify, prevent, and/or monitor criminal and terrorist activity." This strongly implies the use of statistical dragnets that have come to be called data-mining. The inevitable result of a data-mining approach to fusion centers will be:
>
> Many innocent individuals will be flagged, scrutinized, investigated, placed on

> watch lists, interrogated or arrested, and possibly suffer irreparable harm to their reputation, all because of a hidden machinery of data brokers, information aggregators and computer algorithms.
>
> Law enforcement agencies will waste time and resources investing in high-tech computer boondoggles that leave them chasing false leads–while real threats go unaddressed and limited resources are sucked away from the basic, old-fashioned legwork that is the only way genuine terror plots have ever been foiled. (Michael German and Jay Staley, "What's Wrong with Fusion Centers," American Civil Liberties, December 2007)

But perhaps "high-tech computer boondoggles" are *precisely the point!*

After all, the **Boeing Company** and their sidekicks at **SRI International** (which describes itself as "an independent, nonprofit research institute") were recently criticized by a House Science and Technology Subcommittee for "irregularities" in the government's Railhead program, a suite of software "upgrades" to the Terrorist Identities Datamart Environment (TIDE), "a vast database of names that feeds the nation's terrorist watch list," the ***Associated Press*** reported.

Railhead was touted as a "fix" for a system built by Lockheed Martin in the wake of the 9/11 terror attacks. According to congressional investigators, the system provides data to all federal terrorist watch lists, including the "no-fly" list run by the Department of Homeland Security's Transportation Security Administration and the FBI's Terrorist Screening Center, a national clearinghouse for federal, state and local fusion centers.

According to the House committee the program is months behind schedule, millions over budget and "would actually be less capable than the U.S. government terrorist tracking system it is meant to replace." Last week, *The Wall Street Journal* **reported**,

> When tested, the new system failed to find matches for terrorist-suspect names that were spelled slightly different from the name entered into the system, a common challenge when translating names from Arabic to English. It also could not perform basic searches of multiple words connected with terms such as "and" and "or." (Siobhan Gorman, "Flaws Found in Watch List for Terrorists, The Wall Street Journal, August 22, 2008)

Leaving aside the racist presuppositions of the *Journal*, to wit, that Arab = terrorist (no small matter when dealing with nativist yahoos here in the "homeland" or elswehere), as Rep. Brad Miller (D-N.C.) said in a statement, "the program appears to be on the brink of collapse after an estimated half-billion dollars in taxpayer funding has been spent on it." According to the **committee**,

> The Railhead program had been undergoing an internal technical implosion for more than one year. But public statements and sworn public testimony to Congress from senior officials within the NCTC [National Counterterrorist Center] and the Office of the Director of National Intelligence (ODNI) never revealed the mounting technical troubles, poor contractor management or lax government oversight that appears to have been endemic throughout the program and has led to Railhead's colossal failure. Astoundingly, the Director of NCTC and the Director of National Intelligence have both specifically pointed to TIDE and NCTC Online as hallmarks of the government's information sharing accomplishments. ("Technical Flaws Hinder Terrorist Watch List; Congress Calls

for Investigation," Committee on Science and Technology, Press Release, August 21, 2008)

In a *technical sense*, the NCTC and the ODNI may be correct in touting TIDE and NCTC Online as "hallmarks of the government's information sharing accomplishments," *if* by "sharing accomplishments" they meant handing over unlimited bundles of taxpayer's hard-earned cash to enterprising contractors!

Gorman reports that in "recent weeks, the government has fired most of the 862 private contractors from dozens of companies working on the Railhead project, and only a skeleton crew remains." Boeing and SRI's response? According to the *Journal*, "calls to officials of Boeing and SRI were not immediately returned."

I bet they weren't! Especially since the committee said "Railhead insiders" allege that the government paid Boeing some $200 million to retrofit the company's Herndon, Virginia office with security upgrades so that top secret software work could be performed there. The government then leased the *same* office space from Boeing. How's that for hitting the old corporate "sweet spot."

None of this of course, should surprise anyone, least of all defense lobby dollar-addicted members of Congress who, like Captain Renault in *Casablanca* are "shocked, shocked" to find their corporate "partners" have failed to deliver–again.

According to *Washington Technology's* **list** of "2008 Top 100 Government Prime Contractors," Boeing clocked-in at No. 2 with $9,706,621,413 in taxpayer handouts. No slouches themselves, Siemens placed No. 79 with some $186,292,146 in prime government contracts across an array of defense and civilian agencies. With Railhead's imminent demise, perhaps the German electronics giant has a future in the U.S. "homeland security" market with its Intelligent Platform?

Then again, perhaps not. Computer security expert Bruce Schneier told *New Scientist*, "'currently there are no good patterns available to recognise terrorists,' he says, and questions whether Siemens has got around this." But since the business of government is business, maybe they do after all.

Meanwhile, the **PRISE** consortium of security technology and human rights experts funded by the European Union, called "for a moratorium on the development of fusion technologies, referring explicitly to the Siemens Intelligence Platform," Margottini reported.

According to *New Scientist*, PRISE analysts told the EU, "The efficiency and reliability of such tools is as yet unknown. More surveillance does not necessarily lead to a higher level of societal security. Hence there must be a thorough examination of whether the resulting massive constraints on human rights are proportionate and justified."

But here in the United States concern over trivial things such as "massive constraints on human rights," unlike state attacks against the "quaint" rights of the average citizen are, like the impeachment of a regime studded with war criminals, most definitely "off the table."

While the Democrats celebrate Barack Obama's coronation in Denver this week and the Republicans are poised to do the same for John McCain in the Twin Cities rest assured,

administrations may change, *but the corporate grift is eternal*.

Tom Burghardt *is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly, Love & Rage and Antifa Forum, he is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by* ***AK Press***.

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