GlobalResearch
Center for Research on Globalization

Spying on Individuals and Organizations: Anglo-American Defense Giants Entrusted with "Mastering the Internet"

By Tom Burghardt
Global Research, May 08, 2009
Antifascist Calling 8 May 2009

Theme: Intelligence, Police State & Civil Rights

The Government Communications Headquarters (GCHQ), the National Security Agency's "kissin' cousin" across the Atlantic pond, has awarded a £200m ($300m U.S.) contract for an internet panopticon.

American defense and security giant Lockheed Martin and BAE subsidiary Detica (yet another firm specializing "in collecting, managing and exploiting information to reveal actionable intelligence"), snagged the contract The Register and The Sunday Times revealed May 3.

According to The Register the new system, called Mastering the Internet (MTI) "will include thousands of deep packet inspection probes inside communications providers' networks, as well as massive computing power at the intelligence agency's Cheltenham base, 'the concrete doughnut'."

Lockheed Martin and Detica aren't talking and have referred all inquiries on the MTI contract to GCHQ. ComputerWeekly however, reported May 6 that Detica, a firm with close ties to MI5 and MI6, "has data mining software that can detect links between individuals based on their contacts with sometimes widely separated organisations."

The magazine revealed in 2007 that the Insurance Fraud Bureau (IFB) "has outsourced its data mining operations to Detica, a specialist IT company. Its NetReveal software applies social network analysis to huge amounts of data to identify, understand, and evaluate higher-level networks of potentially collusive individuals and organisations."

It would appear the system under construction by GCHQ will apply a similarly unsound and unscientific approach to "counterterrorism." As the National Research Council revealed in their 2008 report on data mining and other dodgy methodologies such as link- and social network analysis for reading digital tea leaves, such techniques "are likely to generate huge numbers of false leads."

However, as a repressive tool for corralling recalcitrant individuals such as antiwar campaigners, environmental activists, socialists and Muslims under Britain's draconian 2006 Terrorism Act, thousands of digital nodes designed to "master the internet" would certainly fit the bill for spooks-gone-wild.

While £200m is a lot of boodle to spy and data mine the private communications and internet browsing habits of British citizens, as James Bamford revealed in Body of Secrets,

GCHQ is a key member of the exclusive "UKUSA club."

Under terms of the Cold War-era UKUSA Communications Intelligence Agreement, a surveillance nexus linking the United States, Canada, Britain, Australia and New Zealand, a cosy relationship was created where member agencies agreed to share information, including that obtained illegally on their citizens, with one another. "By the late 1980s," Bamford wrote, "there was barely a corner of the earth not covered by a listening post belonging to one of the members, or by an American satellite."

GCHQ whistleblower Katherine Gun revealed in 2004, that British spooks and their American partners at NSA had sought leverage by spying on diplomats at the United Nations during the run-up to the U.S.-led invasion and occupation of Iraq, The Observer reported.

A firestorm of protest erupted in the usually staid confines of the UN Security Council when Gun leaked a memo to The Observer from NSA section leader Frank Koza to his compadres at GCHQ. The missive detailed a massive spying operation designed to give America "the edge" in forthcoming negotiations over a second UN resolution authorizing war–and what NSA expected from GCHQ. Despite their efforts the targeted nations–Chile, Pakistan, Guinea, Angola, Cameroon and Bulgaria–wouldn't play ball.

It now appears that GCHQ has expanded its brief and intends to routinely spy on British internet users under the guise of "preventing terrorism." According to The Register,

> Sources said MTI received approval and funding of more than £1bn over three years in the October 2007 Comprehensive Spending Review. GCHQ, like MI5 and MI6, is funded out of the opaque Single Intelligence Account. For 2007/8 the planned budget for the three agencies was over £1.6bn.
>
> GCHQ began work on MTI soon after it was approved. Records of job advertising by the agency show that in April 2008 it was seeking a Head of Major Contracts with "operational responsibility for the 'Mastering the Internet' (MTI) contract". The new senior official was to be paid an annual salary of up to £100,000. (Chris Williams, "Jacqui's secret plan to 'master the internet'," The Register, May 3, 2009)

Not to be outdone by NSA's all-inclusive driftnet surveillance of American citizens, The Sunday Times reported that "the £1 billion snooping project … will rely on thousands of 'black box' probes being covertly inserted across online infrastructure."

> The top-secret programme began to be implemented last year, but its existence has been inadvertently disclosed through a GCHQ job advertisement carried in the computer trade press.
>
> Last week, in what appeared to be a concession to privacy campaigners, Smith announced that she was ditching controversial plans for a single "big brother" database to store centrally all communications data in Britain.
>
> "The government recognised the privacy implications of the move [and] therefore does not propose to pursue this move," she said.
>
> Grabbing favourable headlines, Smith announced that up to £2 billion of public money would instead be spent helping private internet and telephone companies to retain information for up to 12 months in separate databases.

> However, she failed to mention that substantial additional sums–amounting to more than £1 billion over three years–had already been allocated to GCHQ for its MTI programme. (David Leppard and Chris Williams, "Jacqui Smith's secret plan to carry on snooping," The Sunday Times, May 3, 2009)

When news of GCHQ's project surfaced, the director of Liberty, Shami Chakrabarti, said Smith's announcement was a "smokescreen" meant to conceal the new MTI project. The civil liberties' watchdog group had applauded the Home Secretary's apparent "climb-down" on an earlier proposal for a a centralized communications database.

Chakrabarti told The Sunday Times, "We opposed the big brother database because it gave the state direct access to everybody's communications. But this network of black boxes achieves the same thing via the back door." One might add, seamlessly and silently through deep packet inspections of message content.

A deep packet inspection refers to a form of computer network filtering that examines the data portion of a communication (including a message header) as it passes the inspection point of an ISP. While it can filter out viruses and spam, the technology can also enable advanced security functions such as data mining, internet eavesdropping and censorship.

Additionally, because ISP's route all of their customers' traffic to a multitude of network providers, they are also able to monitor web-browsing habits in a way that permit them to gain insight into their customers' interests; this then, becomes the basis of a new form of corporate grift: the sale of data to companies that specialize in targeted advertising.

In the United States for example, NSA's unholy alliance with AT&T, Verizon and other giant telecommunications companies, use deep packet inspection to facilitate internet surveillance, sorting and forwarding private communications to a multitude of spooky agencies.

As the Electronic Frontier Foundation has documented in their landmark lawsuits against telecommunications' grifters and the state, Hepting v. AT&T and Jewel v. NSA, AT&T's suite of "secret rooms" located across the country function as virtual–and illegal–NSA listening posts.

According to AT&T whistleblower Mark Klein, the NSA's SG3 secure room is where internet traffic is split and then diverted to NSA worker ants, most likely outsourced techno-drones hired by the agency to do the dirty work. Private communications are then analyzed by Narus traffic analyzers and logic servers. Narus, a spooky Israeli corporation with a Mountain View, California address as a "beard," claims that its devices are capable of real-time data collection and capture at 10 gigabits per second.

In his sworn affidavit Klein told the Court:

> Starting in February 2003, the "splitter cabinet" split (and diverted to the SG3 Secure Room) the light signals that contained the communications in transit to and from AT&T's Peering Links with the following Internet networks and Internet exchange points: ConXion, Verio, XO, Genuity, Quest, PAIX, Allegiance, Abovenet, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet, and MAE-West.
>
> Internet exchange points are facilities at which large numbers of major Internet

> service providers interconnect their equipment in order to facilitate the communications among their respective networks.
>
> Through the "splitter cabinet," the content of all the electronic voice and data communications going across the Peering Links … was transferred from the WorldNet Internet room's fiber optical circuits into the SG3 Secure Room. ("Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction," United States District Court, Northern District of California, Hepting v. AT&T, No. C-06-0672-VRW, March 28, 2006)

According to Wired, the Narus STA 6400 Semantic Traffic Analyzer "can keep track of, analyze and record nearly every form of internet communication, whether e-mail, instant message, video streams or VOIP phone calls that cross the network."

The system under construction by GCHC may surpass the already-intrusive Big Brother capabilities of NSA. Indeed, GCHQ under terms of the UKUSA Communications Intelligence Agreement may in fact be building the system in cahoots with NSA. Certainly the presence of Lockheed Martin would indicate something more than a simple business deal with British spooks!

Suffice it to say, a source familiar with GCHQ's Mastering the Internet project told The Register, "In MTI, computing resources are not measured by the traditional capacities or speeds such as Gb, Tb, Megaflop or Teraflop… but by the metric tonne!.. and they have lots of them."

As author James Bamford points out in his essential book, The Shadow Factory, NSA is currently researching–and racing–to deploy supercomputers with exaflop capacities (one quintillion operations per second); it wouldn't be a stretch to infer that American spies may very well be assisting their British counterparts in a deranged quest to field the next generation of monstrous data mining and surveillance machines.

But don't be alarmed. Just like their American partners, GCHQ operates with "strict accountability … under the existing legal framework." In response to media reports, GCHQ issued a press release May 3 claiming,

> Because we rely upon maintaining an advantage over those that would damage UK interests, it is usually the case that we will not disclose information about our operations and methods. People sometimes assume that secrecy comes at the price of accountability but nothing could be further from the truth. In fact, GCHQ is subject to rigorous parliamentary and judicial oversight (the Intelligence and Security Committee of parliamentarians, and two senior members of the judiciary: the Intelligence Services Commissioner and the Interception of Communications Commissioner) and works entirely within a legal framework that complies with the European Convention on Human Rights. ("GCHQ: Our Intelligence and Security mission in the Internet Age," Government Communications Headquarters, Press Release, May 3, 2009)

Try selling that to countless victims of the 1994 Intelligence Services Act or the 2000 Regulation of Investigatory Powers Act. After all, as public servants at the beck and call of their political and corporate masters, "GCHQ does not spy at will"!

The original source of this article is Antifascist Calling

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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