

Big Ears and Big Secrets

European Officials Suspect the United States is Spying on Its Allies

By David Ruppe

NEW YORK, July 16 —Some of America's closest European allies suspect a massive U.S. listening post, nestled on the quiet, windswept moors of northern England, has secretly been spying on European governments, businesses and citizens.

The station, located at Menwith Hill in Yorkshire, and reportedly staffed with more than 1,000 Americans, was created nearly 40 years ago to keep tabs on the Soviet empire.

But since the Cold War, the station has continued to expand, reportedly adding billions of dollars worth of sophisticated listening equipment capable of simultaneously intercepting millions of European telephone conversations, faxes and e-mails.

The more than two-dozen “radomes” now visible at the site — giant golf-ball like structures containing satellite dishes and other listening equipment — are used to download information from U.S. spy satellites and intercept communications relayed through commercial satellites from Europe, North Africa and western Asia, experts say.

The site is supposed to be used to monitor matters of international security, such as weapons proliferation, drug trafficking and terrorism. But according to numerous European press reports, businesses, civil liberties groups, and some government officials believe Menwith Hill and a sister post at Bad Aibling, Germany are also targeting them.

Suspicious of Spying

A report released by the European Parliament in 1998 further stirred up fears of illegal eavesdropping. It concluded Menwith Hill and a related system of sites are “designed for primarily non-military targets: governments, organizations and businesses in virtually every country.”

“French law forbids that kind of interception,” says David Nataf, a French lawyer for an organization representing defense, aerospace and telecommunications companies.

Since the report, legislators have pressured the French government to explain what it was doing to counter Menwith Hill’s capabilities, Nataf says.

Through the UKUSA alliance, the U.S., Britain, Canada, Australia and New Zealand monitor phone, fax, e-mail and other communications worldwide. Communications satellite listening posts intercept signals passing through commercial and other satellites. U.S. SIGINT (signals intelligence) posts collect information intercepted by spy satellites.

(ABCNEWS.com/ Magellan Geographix)

In response, he says, the French government last March issued a decree allowing the public to use more powerful encryption, which would hamper eavesdropping on, say, e-mail and telephone conversations.

Germany last month also announced it would relax encryption controls and took the unusual step of announcing it would promote the use of powerful encryption throughout Germany — even though both moves will likely make eavesdropping by

law enforcement more difficult.

Neither government mentioned U.S. intelligence gathering as a reason, though each alluded to a growing threat of espionage against national businesses and citizens.

In Britain, the government has been asked repeatedly to provide assurances that operations at Menwith Hill are not breaking the law.

In March, a British member of Parliament queried his government on whether U.S. activities at Menwith Hill fully comply with British law, U.S. law, European Union law, and international law.

Not really answering the question, the government responded: “The United States Visiting Forces authorities...at RAF Menwith Hill, are required to respect the laws of this country.”

Damaging European Report

Then, in April, the European Parliament released a report specifically charging that the U.S. government used information gained through eavesdropping during international trade negotiations, and that U.S. companies used it, too, to defeat European competitors in major trade competitions.

The report, authored by British investigative journalist Duncan Campbell, cited several news accounts of alleged economic espionage, including a 1995 story in *The Baltimore Sun*.

“Former intelligence officials and other experts say tips based on spying... regularly flow from the Commerce Department to U.S. companies to help them win contracts overseas,” the *Sun* reported.

The report said the Commerce Department, which is responsible for promoting U.S. trade, has an office specially designated to receive information from the intelligence community.

It also charged that Internet browsers and other software shipped to Europe by American manufacturers are intentionally disabled so secure communications can be read by the U.S. National Security Agency, the cornerstone organization of U.S. electronic intelligence, without difficulty.

Since the report’s release, Sweden’s foreign minister has said his government will investigate whether Swedish companies were harmed by American spying. Another British MP has called on his government to stop Menwith Hill from spying on British companies and citizens.

The NSA refused to comment on Menwith Hill.

A Global System

The two European Parliament reports and two decades of investigative reporting have established that Menwith Hill and Bad Aibling form part of a scheme of more than a dozen major listening posts operated around the world by the United States, Britain, Canada, Australia and New Zealand through a semi-secret alliance called “UKUSA.”

The sites are linked by a system known as “ECHELON,” through which the countries collect, select and deliver to each other information intercepted from communications worldwide.

The NSA also refuses to discuss UKUSA.

Governments Silent

Still, despite all the suspicions, no European government has, at least publicly, protested UKUSA's suspected eavesdropping.

Were the issue to be raised at the national level, it would likely occur through the European Union, says Simon Davies, UK director of the watchdog group Privacy International.

"If the level of commercial espionage is as it has been suggested in the European Parliament's report, then both the [European Union's] Maastricht and the Amsterdam treaties are being fundamentally violated by Great Britain, and possibly Germany," he says.

But because the United States shares some intelligence with other governments, it is not clear what country would bring a case, says Davies. "The Catch-22 is that governments aren't going to take action on ECHELON or any of the other NSA programs, because they are in such collusion with the NSA."

Other countries outside the UKUSA alliance, such as Russia, Germany and France, also are believed to operate their own, albeit less sophisticated, eavesdropping facilities around the globe, and so also may be reluctant to point fingers.

Another problem, observers say, is that the ECHELON program has never been acknowledged by the United States or Britain. "France can't ask for an assurance on something that is not official," says a French government official.

Exaggerated Concerns?

By the nature of National Security Agency's technology — which sweeps in all manner of communications from commercial satellites, spy satellites and other means—it is inevitable the agency will intercept messages European companies and citizens consider confidential, experts say.

But some are not convinced the agency is extracting, analyzing and sharing with U.S. companies such information to any significant degree, if at all.

"The concerns of the European community are a bit overblown," says James Bamford, author of *The Puzzle Palace*, the definitive book on the NSA.

"The [NSA is] not worried about some company in Brussels. They're worried about the things you see on the front page of *The Washington Post* and *The New York Times*, terrorism, Kosovo."

Steve Aftergood, director of the project on government secrecy at the Federation of American Scientists in Washington, agrees. "I don't know that to be the case, namely, that industrial espionage is a policy of the U.S. intelligence community."

The United States does collect "various kinds of photographic, signals, political and other intelligence," Aftergood says, but he asserts the economic intelligence collected by U.S. spy agencies focuses more on "what is going on in markets, emerging markets, where resources are being identified and discovered."

However, Duncan Campbell, the author of the European Parliament's April report, doesn't believe any of that for a minute. "Everybody does this. It's a surprise to me that anybody thinks it's a surprise," he says.

"Yes, [U.S. spying] includes market trends but it doesn't stop there. If you are going to determine economic trends in a fast moving economic situation other than reading *The Wall Street Journal* and *The Financial Times*, how are you going to do it? By spying on contractual negotiations as they happen." —