Breaking the Taboo on Israel's Spying Efforts on the United States

Christopher Ketchamd
Atlantic Free Press
12 March 2009
http://atlanticfreepress.com/news/1/8528-breaking-the-taboo-on-israels-spying-efforts-on-the-united-states.html

> Israel runs one of the most aggressive and damaging espionage networks targeting the U.S., yet public discussion about it is almost nil. Scratch a counterintelligence officer in the U.S. government and they'll tell you that Israel is not a friend to the United States.

This is because Israel runs one of the most aggressive and damaging espionage networks targeting the U.S.. The fact of Israeli penetration into the country is not a subject oft-discussed in the media or in the circles of governance, due to the extreme sensitivity of the U.S.-Israel relationship coupled with the burden of the Israel lobby, which punishes legislators who dare to criticize the Jewish state. The void where the facts should sit is filled instead with the hallucinations of conspiracy theory — the kind in which, for example, agents of the Mossad, Israel's top intelligence agency, engineer the 9/11 attacks, while 4,000 Israelis in the Twin Towers somehow all get word to escape before the planes hit. The effect, as disturbing as it is ironic, is that the less the truth is addressed, the more noxious the falsity that spreads.

Israel's spying on the U.S., however, is a matter of public record, and neither conspiracy nor theory is needed to present the evidence. When the FBI produces its annual report to Congress concerning "Foreign Economic Collection and Industrial Espionage," Israel and its intelligence services often feature prominently as a threat second only to China. In 2005 the FBI noted, for example, that Israel maintains "an active program to gather proprietary information within the United States." A key Israeli method, said the FBI report, is computer intrusion. In 1996, the Defense Intelligence Service, a branch of the Pentagon, issued a warning that "the collection of scientific intelligence in the United States [is] the third highest priority of Israeli Intelligence after information on its Arab neighbors and information on secret U.S. policies or decisions relating to Israel." In 1979, the Central Intelligence Agency produced a scathing survey of Israeli intelligence activities that targeted the U.S. government. Like any worthy spy service, Israeli intelligence early on employed wiretaps as an effective tool, according to the CIA report. In 1954, the U.S. Ambassador in Tel Aviv discovered in his office a hidden microphone "planted by the Israelis," and two years later telephone taps were found in the residence of the U.S. military attaché. In a telegram to Washington, the ambassador at the time cabled a warning: "Department must assume that all conversations [in] my office are known to the Israelis." The former ambassador to Qatar, Andrew Killgore, who also served as a foreign officer in Jerusalem and Beirut, told me Israeli taps of U.S. missions and embassies in the Middle East were part of a "standard operating procedure."

According to the 1979 CIA report, the Israelis, while targeting political secrets, also devote "a considerable portion of their covert operations to obtaining scientific and technical intelligence." These operations involved, among other machinations, "attempts to penetrate certain classified defense projects in the United States." The penetrations, according to the CIA report, were effected using "deep cover enterprises," which the report described as "firms and organizations, some specifically created for, or adaptable to, a specific objective." At the time, the CIA singled out government-subsidized companies such as El Al airlines and Zim, the Israeli shipping firm,

as deep cover enterprises. Other deep cover operations included the penetration of a U.S. company that provided weapons-grade uranium to the Department of Defense during the 1960s; Israeli agents eventually spirited home an estimated 200 pounds of uranium as the bulwark in Israel's secret nuclear weapons program. Moles have burrowed on Israel's behalf throughout the U.S. intelligence services. Perhaps most infamous was the case of Jonathan Pollard, a Jewish-American employed as a civilian analyst with the U.S. Navy who purloined an estimated 800,000 code-word protected documents from inside the CIA, the Defense Intelligence Agency, and numerous other U.S. agencies. While Pollard was sentenced to life in prison, counterintelligence investigators at the FBI suspected he was linked to a mole far higher in the food chain, ensconced somewhere in the DIA, but this suspected Israeli operative, nicknamed "Mr. X," was never found. Following the embarrassment of the Pollard affair — and its devastating effects on U.S. national security, as testified by then Defense Secretary Caspar Weinberger (who allegedly stated that Pollard "should have been shot") — the Israeli government vowed never again to pursue espionage against its ally and chief benefactor.

Fast-forward a quarter century, and the vow has proven empty. In 2004, the authoritative Jane's Intelligence Group noted that Israel's intelligence organizations "have been spying on the U.S. and running clandestine operations since Israel was established." The former deputy director of counterintelligence at FBI, Harry B. Brandon, last year told Congressional Quarterly magazine that "the Israelis are interested in commercial as much as military secrets. They have a muscular technology sector themselves." According to CQ, "One effective espionage tool is forming joint partnerships with U.S. companies to supply software and other technology products to U.S. government agencies."

Best-selling author James Bamford now adds another twist in this history of infiltration in a book published last October, "The Shadow Factory," which forms the latest installment in his trilogy of investigations into the super-secret National Security Agency. Bamford is regarded among journalists and intelligence officers as the nation's expert on the workings of the NSA, whose inner sanctums he first exposed to the public in 1982. (So precise is his reporting that NSA officers once threw him a book party, despite the fact that he continually reveals their secrets.) The agency has come a long way in the half-century since its founding in 1952. Armed with digital technology and handed vast new funding and an almost limitless mandate in the wake of the 9/11 attacks, Bamford writes, the NSA has today "become the largest, most costly, and most technologically sophisticated spy organization the world has ever known." The NSA touches on every facet of U.S. communications, its mega-computers secretly filtering "millions of phone calls and e-mails" every hour of operation. For those who have followed the revelations of the NSA's "warrantless wiretapping" program in the New York Times in 2005 and the Wall Street Journal last year, what Bamford unveils in "The Shadow Factory" is only confirmation of the worst fears: "There is now the capacity," he writes of the NSA's tentacular reach into the private lives of Americans, "to make tyranny total."

Much less has been reported about the high-tech Israeli wiretapping firms that service U.S. telecommunications companies, primarily AT&T and Verizon, whose networks serve as the chief conduits for NSA surveillance. Even less is known about the links between those Israeli companies and the Israeli intelligence services. But what Bamford suggests in his book accords with the history of Israeli spying in the U.S.: Through joint partnerships with U.S. telecoms, Israel may be a shadow arm of surveillance among the tentacles of the NSA. In other words,

when the NSA violates constitutional protections against unlawful search and seizure to vacuum up the contents of your telephone conversations and e-mail traffic, the Israeli intelligence services may be gathering it up too — a kind of mirror tap that is effectively a two-government-in-one violation.

***

On its face, the overseas outsourcing of high-tech services would seem de rigueur in a competitive globalized marketplace. Equipment and services from Israel's telecom sector are among the country's prime exports, courtesy of Israeli entrepreneurs who have helped pioneer wireless telephony, voicemail and voice recognition software, instant messaging, phone billing software, and, not least, "communications interception solutions." Israeli telecom interception hardware and software is appraised as some of the best in the world.

By the mid-1990s, Israeli wiretap firms would arrive in the U.S. in a big way. The key to the kingdom was the 1994 Communications Assistance for Law Enforcement Act (CALEA), which was Congress' solution for wiretapping in the digital age. Gone are the days when wiretaps were conducted through on-site tinkering with copper switches. CALEA mandated that telephonic surveillance operate through computers linked directly into the routers and hubs of telecom companies — a spyware apparatus matched in real-time, all the time, to American telephones and modems. CALEA effectively made spy equipment an inextricable ligature in telephonic life. Without CALEA, the NSA in its spectacular surveillance exploits could not have succeeded.

AT&T and Verizon, which together manage as much as 90 percent of the nation's communications traffic, contracted with Israeli firms in order to comply with CALEA. AT&T employed the services of Narus Inc., which was founded in Israel in 1997. It was Narus technology that AT&T whistleblower Mark Klein, a 22-year technician with the company, famously unveiled in a 2006 affidavit that described the operations in AT&T's secret tapping room at its San Francisco facilities. (Klein's affidavit formed the gravamen of a lawsuit against AT&T mounted by the Electronic Freedom Foundation, but the lawsuit died when Congress passed the telecom immunity bill last year.) According to Klein, the Narus supercomputer, the STA 6400, was "known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for preprogrammed targets." The Narus system, which was maintained by Narus technicans, also provided a real-time mirror image of all data streaming through AT&T routers, an image to be rerouted into the computers of the NSA.

According to Jim Bamford, who cites knowledgeable sources, Verizon's eavesdropping program is run by a competing Israeli firm called Verint, a subsidiary of Comverse Technology, which was founded by a former Israeli intelligence officer in 1984. Incorporated in New York and Tel Aviv, Comverse is effectively an arm of the Israeli government: 50 percent of its R&D costs are reimbursed by the Israeli Ministry of Industry and Trade. The Verint technology deployed throughout Verizon's network, known as STAR-GATE, boasts an array of Orwellian capabilities. "With STAR-GATE, service providers can access communications on virtually any type of network," according to the company's literature. "Designed to manage vast numbers of targets, concurrent sessions, call data records, and communications, STAR-GATE transparently accesses targeted communications without alerting subscribers or disrupting service." As with the Narus system, the point is to be able to tap into communications unobtrusively, in real time,

all the time. A Verint spinoff firm, PerSay, takes the tap to the next stage, deploying "advanced voice mining," which singles out "a target's voice within a large volume of intercepted calls, regardless of the conversation content or method of communication." Verint's interception systems have gone global since the late 1990s, and sales in 2006 reached $374 million (a doubling of its revenues over 2003). More than 5,000 organizations — mostly intelligence services and police units — in at least 100 countries today use Verint technology.

What troubles Bamford is that executives and directors at companies like Narus and Verint formerly worked at or maintain close connections with the Israeli intelligence services, including Mossad; the internal security agency Shin Bet; and the Israeli version of the NSA, Unit 8200, an arm of the Israeli Defense Forces Intelligence Corps. Unit 8200, which Bamford describes as "hypersecret," is a key player in the eavesdropping industrial complex in Israel, its retired personnel dispersed throughout dozens of companies. According to Ha'aretz, the Israeli daily, "Many of the [eavesdropping] technologies in use around the world and developed in Israel were originally military technologies and were developed and improved by [Unit 8200] veterans." A former commander of Unit 8200, cited by Bamford, states that Verint technology was "directly influenced by 8200 technology….[Verint parent company] Comverse's main product, the Logger, is based on the Unit's technology." The implications for U.S. national security, writes Bamford, are "unnerving." "Virtually the entire American telecommunications system," he avers, "is bugged by [Israeli-formed] companies with possible ties to Israel's eavesdropping agency." Congress, he says, maintains no oversight of these companies' operations, and even their contracts with U.S. telecoms — contracts pivotal to NSA surveillance — are considered trade secrets and go undisclosed in company statements.

U.S. intelligence officers have not been quiet in their concerns about Verint (I reported on this matter in CounterPunch.org last September). "Phone calls are intercepted, recorded, and transmitted to U.S. investigators by Verint, which claims that it has to be 'hands on' with its equipment to maintain the system," says former CIA counterterrorism officer Philip Giraldi. The "hands on" factor is what bothers Giraldi, specifically because of the possibility of a "trojan" embedded in Verint wiretap software. A trojan in information security hardware/software is a backdoor that can be accessed remotely by parties who normally would not have access to the secure system. Allegations of widespread trojan spying have rocked the Israeli business community in recent years. "Top Israeli blue chip companies," reported the AP in 2005, "are suspected of using illicit surveillance software to steal information from their rivals and enemies." Over 40 companies have come under scrutiny. "It is the largest cybercrime case in Israeli history," Boaz Guttmann, a veteran cybercrimes investigator with the Israeli national police, told me. "Trojan horse espionage is part of the way of life of companies in Israel. It's a culture of spying."

In a wide-ranging four-part investigation into Israel-linked espionage that aired in December 2001, Carl Cameron, a correspondent at Fox News Channel, reported the distress among U.S. intelligence officials warning about possible trojans cached in Verint technology. Sources told Cameron that "while various FBI inquiries into [Verint] have been conducted over the years," the inquiries had "been halted before the actual equipment has ever been thoroughly tested for leaks." Cameron also cited a 1999 internal FCC document indicating that "several government agencies expressed deep concerns that too many unauthorized non-law enforcement personnel can access the wiretap system." Much of this access was facilitated through "remote

maintenance."

The Fox News report reverberated throughout U.S. law enforcement, particularly at the Drug Enforcement Agency, which makes extensive use of wiretaps for narcotics interdiction. Security officers at DEA, an adjunct of the Justice Department, began examining the agency's own relationship with Comverse/Verint. In 1997, DEA had transformed its wiretap infrastructure with the $25 million procurement from Comverse/Verint of a technology called "T2S2" — "translation and transcription support services" — with Comverse/Verint contracted to provide the hardware and software. The company was also tasked with "support services, training, upgrades, enhancements and options throughout the life of the contract," according to the DEA's "contracts and acquisitions" notice. In the wake of the Fox News investigation, however, the director of security programs at DEA, Heidi Raffanello, was rattled enough to issue an internal communiqué on the matter, dated Dec. 18, 2001. Directly referencing Fox News, she worried that "Comverse remote maintenance" was "not addressed in the C&A [contracts and acquisitions] process….It remains unclear if Comverse personnel are security cleared, and if so, who are they and what type of clearances are on record….Bottom line we should have caught it." It is not known what resulted from DEA's review of the issue of remote maintenance and access by Comverse/Verint.

Bamford devotes a portion of his argument to the detailing of the operations of a third Israeli wiretap company, NICE Systems, which he describes as "a major eavesdropper in the U.S." that "keeps its government and commercial client list very secret." Formed in 1986 by seven veterans of Unit 8200, NICE software "captures voice, email, chat, screen activity, and essential call details," while offering "audio compression technology that performs continuous recordings of up to thousands of analog and digital telephone lines and radio channels." NICE Systems has on at least one occasion shown up on the radar of U.S. counterintelligence. During 2000-2001, when agents at the FBI and the CIA began investigating allegations that Israeli nationals posing as "art students" were in fact conducting espionage on U.S. soil, one of the Israeli "art students" was discovered to be an employee with NICE Systems. Among the targets of the art students were facilities and offices of the Drug Enforcement Agency nationwide. The same Israeli employee of NICE Systems, who was identified as a former operative in the Israeli intelligence services, was carrying a disk that contained a file labeled "DEA Groups." U.S. counterintelligence officers concluded it was a highly suspicious nexus: An Israeli national and alleged spy was working for an Israeli wiretap company while carrying in his possession computer information regarding the Drug Enforcement Agency — at the same time this Israeli was conducting what the DEA described as "intelligence gathering" about DEA facilities.

***

A former senior counterintelligence official in the Bush administration told me that as early as 1999, "CIA was very concerned about [Israeli wiretapping companies]" — Verint in particular. "I know that CIA has tried to monitor what the Israelis were doing — technically watch what they were doing on the networks in terms of remote access. Other countries were concerned as well," said the intelligence official. Jim Bamford, who notes that Verint "can automatically access the mega-terabytes of stored and real-time data secretly and remotely from anywhere," reports that Australian lawmakers in 2004 held hearings on this remote monitoring capability. "[Y]ou can access data from overseas," the lawmakers told a Verint representative during the

hearings, "but [the legislature] seems restricted to access data within that system." The Australians found this astonishing. In 2000, the Canadian intelligence service, the Royal Canadian Mounted Police, conducted "a probe related to allegations that [Israeli] spies used rigged software to hack into Canada's top secret intelligence files," according to an article in the Toronto Star. Several sources in the U.S. intelligence community told me the Canadians liaised with their American counterparts to try to understand the problem. According to the Bush administration official who spoke with me, "the Dutch also had come to the CIA very concerned about what the Israelis were doing with this." The Dutch intelligence service, under contract with Verint, "had discovered strange things were going on — there was activity on the network, the Israelis uploading and downloading stuff out of the switches, remotely, and apparently using it for their own wiretap purposes. The CIA was very embarrassed to say, 'We have the same problem.' But the CIA didn't have an answer for them. 'We hear you, we're surprised, and we understand your concern.'" Indeed, sources in the Dutch counterintelligence community in 2002 claimed there was "strong evidence that the Israeli secret service has uncontrolled access to confidential tapping data collected by the Dutch police and intelligence services," according to the Dutch broadcast radio station Evangelische Omroep (EO). In January 2003, the respected Dutch technology and computing magazine, C'T, ran a follow-up to the EO story, headlined "Dutch Tapping Room not Kosher." The article states: "All tapping equipment of the Dutch intelligence services and half the tapping equipment of the national police force [is] insecure and is leaking information to Israel."

"The key to this whole thing is that Australian meeting," Bamford told me in a recent interview. "They accused Verint of remote access and Verint said they won't do it again — which implies they were doing it in the past. It's a matter of a backdoor into the system, and those backdoors should not be allowed to exist. You can tell by the Australian example that it was certainly a concern of Australian lawmakers."

Congress doesn't seem to share the concern. "Part of the responsibility of Congress," says Bamford, "is not just to oversee the intelligence community but to look into the companies with which the intelligence community contracts. They're just very sloppy about this." According to the Bush administration intelligence official who spoke with me, "Frustratingly, I did not get the sense that our government was stepping up to this and grasping the bull by the horns." Another former high level U.S. intelligence official told me, "The fact of the vulnerability of our telecom backbone is indisputable. How it came to pass, why nothing has been done, who has done what — these are the incendiary questions." There is also the fundamental fact that the wiretap technologies implemented by Verint, Narus and other Israeli companies are fully in place and no alternative is on the horizon. "There is a technical path dependence problem," says the Bush administration official. "I have been told nobody else makes software like this for the big digital switches, so that is part of the problem. Other issues," he adds, "compound the problem" — referring to the sensitivity of the U.S.-Israel relationship.

And that, of course, is the elephant in the room. "Whether it's a Democratic or Republican administration, you don't bad-mouth Israel if you want to get ahead," says former CIA counterterrorism officer Philip Giraldi. "Most of the people in the agency were very concerned about Israeli espionage and Israeli actions against U.S. interests. Everybody was aware of it. Everybody hated it. But they wouldn't get promoted if they spoke out. Israel has a privileged position and that's the way things are. It's crazy. And everybody knows it's crazy."