Spies in the Ointment: The Israeli Espionage of Global Communications

By Hei Hu Quan

The Conspiracy Central Blog
July 26, 2007

https://conspiracycentral.wordpress.com/2007/07/26/spies-in-the-ointment-the-israeli-espionage-of-global-communications/

Total Information Awareness, But For Whom?

This story began quite innocuously as a minor retelling of a story I discovered involving an Israeli company called Narus that collects real-time internet information on U.S. citizens for the the U.S. National Security Agency. In the course of my research, the story grew to shocking proportions revealing that the gamut of virtually all electronics communications, **has not only been compromised by a foreign entity within the U.S., but the entire world.** It is an intentional and directed infiltration at effectively every source and core of the scope of electronics communications worldwide. **Rendering all secure systems compromised and intercepted by Israeli security services and for the benefit of using gained intelligence information to their strategic advantages.** The implications, much less the ramifications are staggering, and these bold new revelations have revealed not only a treasonous complicity of the governing host nations, but criminally collusive actions towards a central malevolent end.

Every piece of electronics equipment be it telephone, cellphone, (VoIP) Voice over IP, pagers, Blackberrys, instant messaging services, emails, has a point of interception established by the Israeli intelligence services. **More ominous are the specific inroads these particular groups are making in inserting themselves within strategic centers of security infrastructures within various countries.**

Such as providing direct security for New York's Statue of Liberty, producing communications satellites, creation and management of firewalls for sensitive military & intelligence agencies, and the contract and production of RFID chips with user sensitive data and broadcast abilities for U.S. Passports. Think of that for a moment, especially the encoding for the RFID chips, in which personal data of citizens of the U.S. is in the hands of a foreign national organization with declared loyalties and military allegiances to their home country, along with either simple residencies or dual citizenships that were granted by the U.S. government or host country itself.

In this investigation you will get nowhere if you do not separate Zionism from Judaism in which the former uses as a front, to achieve it's long-standing goals by any and all means. This includes using and manipulating Jewish people in whatever ways they see fit, for to them the ends justify the means.

Bottom line is that we are talking about governments and their puppet-master cabals and orders propagating PSYOPS to manipulate through nationalism, greed and fear. This being said, the government of Israel supports Zionism and the expansion of its goals. But do their people? The corporate governments of the US and UK have open imperialist intentions, reflected in policy and brutality, but do their people condone and support this?

What I am getting at is that people want all the same things in life unless lured and indoctrinated by whatever different flavours the IllumiNazi machine have propagated. These needful things are simple, we all want peace, stability, security and! prosperity for our generations, in a clean, nurturing environment of mutual respect. Those who cannot get aboard this very pure and simple concept, can be said, harbour and support agendas of evil contrary to humanity.

Digression aside, does the Israeli government even give one single fuck about its own people? Or does it use the compulsory military service as an indoctrination system to instil racialist, nationalist and Zionist values; cultivating select young citizens and deploying them globally as spies for empire? The reason I'm positing this is to differentiate between a government that serves the people versus a people whom serve the government against their own personal interests and beliefs.

"Every piece of electronics equipment be it telephone, cellphone, (VoIP) Voice over IP, pagers, Blackberrys, instant messaging services, emails, has a point of interception established by the Israeli intelligence services."

We're going to peer behind the veil and see, that within Israel's military intelligence operations center, there exists compartmentalized intelligence/ spy units to specifically cultivate and train the best and brightest of their army recruits into operatives for electronic espionage and warfare. All have at their heart, and by their own explicit accounts, the development of young military intel operatives that explicitly act as soldier-techs for advanced technological warfare operations. Worse yet is that by utilizing a cover of technological start-up companies, they can not only strategically infiltrate specific targets, and gain access to secure electronics infrastructures, but also use the financial resources garnered to fund their entire operations. It is a truly Trojan horse type operation that must at it's core have collaborative elements within the government that assist and even facilitate these infiltrations.

With that being said, let's examine the principles and entities, their motives and some of their documented areas of interest. The following below are excerpts from sources revealing the background of Israeli military intelligence groups. I shall let the facts speak for themselves. I would also like to add that when writing this, I had my machine hacked into at least 3 times that I am able to confirm absolutely. The first two I tracked and was able to resolve successfully after some particularly invasive system analysis.The last of which specifically attacked this file as I was working on it and deleted a few paragraphs of freshly written material, so all they have done is corroborate that I am on the right track regarding this information and how they view the truth as a threat.

From December 11-14 of 2001, Fox News aired a 4-part special report on Israeli Spying in America, because of it's explosive content and Israel's connections including Rupert Murdoch, the story was not only censored, but all transcripts and video of this story on Fox's website have since been removed and suppressed. A partial transcript and videos for the 4 part series have been preserved here: http://www.whatreallyhappened.com/israeli_spyring_fox.html at whatreallyhappened.com's website. Here's some damning information from the series that substantiate points and allegations raised in this story.

"Since Sept. 11, more than 60 Israelis have been arrested or detained, either under the new patriot anti-terrorism law, or for immigration violations. A handful of active Israeli military were among those detained, according to investigators, who say some of the detainees also failed polygraph questions when asked about alleged surveillance activities against and in the United States.

Numerous classified documents obtained by Fox News indicate that even prior to Sept. 11, as many as 140 other Israelis had been detained or arrested in a secretive and sprawling investigation into suspected espionage by Israelis in the United States.

…

The first part of the investigation focuses on Israelis who say they are art students from the University of Jerusalem and Bazala Academy. They repeatedly made contact with U.S. government personnel, the report says, by saying they wanted to sell cheap art or handiwork. Documents say they, 'targeted and penetrated military bases.' The DEA, FBI and dozens of government facilities, and even secret offices and unlisted private homes of law enforcement and intelligence personnel. The majority of those questioned, 'stated they served in military intelligence, electronic surveillance intercept and or explosive ordinance units.'

…

Another part of the investigation has resulted in the detention and arrests of dozens of Israelis at American mall kiosks, where they've been selling toys called Puzzle Car and Zoom Copter. Investigators suspect a front.

Why would Israelis spy in and on the U.S.? A General Accounting Office investigation referred to Israel as country 'A' and said, 'According to a U.S. intelligence agency, the government of country 'A' conducts the most aggressive espionage operations against the U.S. of any U.S. ally.'

A defense intelligence report said Israel has a voracious appetite for information and said, 'the Israelis are motivated by strong survival instincts which dictate every possible facet of their political and economical policies. It aggressively collects military and industrial technology and the U.S. is a high priority target." The document concludes: 'Israel possesses the resources and technical capability to achieve its collection objectives.'" (Transcript of Fox News Special Report with Brit Hume, from December 11, 2001) - http://www.whatreallyhappened.com/israeli_spyring_fox.html

The Israel Defense Forces (IDF)

"Since the creation of Israel in 1948, the military has compensated for its lack of resources and manpower with brainpower. Particularly in the past 20 years, the IDF has invested billions of dollars in developing technological warfare. The result is a number of secret, semisecret, and open-secret divisions devoted to coming up with cutting-edge technologies designed to help Israel know what its enemies are doing — and to kill them when the need arises. **The units have code names suitable for a spy novel: 8-200, 8153, Mamram, Talpiot, Mamdas.** In the incubator of the IDF, those units, as Israelis winkingly call them, have improved technologies used in everything from digital switching to wireless telephony. Military intelligence elite units, which function as basic training for startup entrepreneurs, are small working groups of highly motivated teams; they work brutal hours and get little sleep; and they face immense pressure to innovate for the sake of national survival. They more than any other single factor are responsible for Israel's technological skills.

American high-tech giants like Cisco, Intel, and Motorola — drawn in no small part by the wealth of technical talent coming out of intelligence units — have set up research facilities in Israel.

Some of Israel's largest and most successful tech companies call the United States home: Comverse, a voice messaging company with a market cap of $14.9 billion, is based in Woodbury, N.Y.; Mercury Interactive is based in Sunnyvale, Calif. More common these days is what's known as the fast exit, whereby startups either sell out to a foreign multinational entirely or split themselves in two, keeping R&D in Israel but moving sales and marketing to the United States." (Startup Nation by Stacy Perman) - http://www.timeinc.net/b2/subscribers/articles/print/0,17925,512689,00.html

"In a more creative sphere, the army and Israeli defense contractors developed the world's first pilotless plane, launched satellites into space, and created a host of other technologies likely never to be revealed." (Israeli Army Grads Lead Business Revolution by David Rosenberg) - http://www.cji.co.il/cji-n126.txt)

Take a close look at this unusually suspicious excerpt from an article entitled: Research Bulletin 72 - The Impact of Globalization on the Boom and Crisis of Israel's High-Tech Industry by B.A. Kipnis. Written in January of 2002, the statements by this D. Globerman are chilling, in the way they convey an almost insider foreknowledge that takes advantage of the post 9/11 chaos and fear. Anticipating an opening and potential investment in anti-terror technologies that can be exploited by Israel to advance their economy and recovery for their High-tech industry. "This might include the upgrading of their technological systems in order to avoid any future terror threat, and the upgrading of the technological capabilities of security agencies, airports, and air companies as well as the military machine needed for the [electronic] war against global terror. These activities, fueled by the spending of many billions of dollars, will help the economy out of its crisis; they will ! be the main driving force behind the likely recovery of the high-tech industry."

*Read the excerpt below and see if this doesn't seem like a bit of an insider smoking gun to you as well.

"At the time of writing the war on global terror is under way and the economic media are busy speculating about the impact of that war, particularly about the effect of the horrible terror event of September 11, 2001 in the US on the world high-tech industry, the Israeli high-tech industry included. D. Globerman, conveyed the emerging stimulators for recovery in the high-tech industry, and the behavior by industry necessary to revive. He cited a 'virtual' pessimist as saying that the current high-tech crisis would not be over before 2003. The cited 'virtual' optimists, on the other hand, would assume that thanks to the vicious September 11 terror attack on the US, the crisis would be over soon because private and public agencies in the US and elsewhere would invest in anti-terror technologies. This might include the upgrading of their technological systems in order to avoid any future terror threat, and the upgrading of the technological capabilities of security agencies,! airports, and air companies as well as the military machine needed for the [electronic] war against global terror. These activities, fueled by the spending of many billions of dollars, will help the economy out of its crisis; they will be the main driving force behind the likely recovery of the high-tech industry. In addition, since the terror has minimized the risk differences between Israel and the rest of the of the developed world, and since there is no place that is 100% safe, investors, holding hot money will eventually look for promising places to invest, including in Israel.

In late September 2001 the Minister of Finance exempted foreign high-tech firms from local company income tax. This ruling is an addition to other grants offered to firms investing in Israel." (Research Bulletin 72 - The Impact of Globalization on the Boom and Crisis of Israel's High-Tech Industry by B.A. Kipnis) - http://www.lboro.ac.uk/gawc/rb/rb72.html

Talpiot

Talpiot is the special army training program that puts the best high school graduates through a rigorous curriculum of computer science, physics, and math, then places them in key assignments in, say, intelligence units. The selection process for Israel's army-trained technology elite starts when teenagers apply to programs, usually in their last two years of high school. Only volunteers are eligible to be chosen for the army's training programs. The most selective program, Talpiot, accepts only 30 applicants, or 1 in 10, a year. Officers say the army doesn't look for fuzzy traits like creativity and leadership; it focuses on measurable qualities. Extremely high aptitude in math and science, along with success in rigorous exams, are the key qualifications.

"The IDF has created special systems to identify the country's best and brightest, and to steer them into the most demanding areas of technological warfare and intelligence work. The elite of the elite pass through a program known as Talpiot, set up in the aftermath of the bloody Yom Kippur War in October 1973. Israel eventually prevailed, but in 18 days of fighting, Egypt and Syria inflicted heavy casualties on the much-vaunted Israeli forces. The idea behind Talpiot, says Major Yariv Danziger, 'was for a unit to gather geniuses in the army to invent new technologies and weapons.' The program was officially started in 1979 with an initial class of 25 "geniuses." Danziger, 34, has headed the program for the past two years.

Think of Talpiot as something like the old East German Olympic athletics program minus the doping. By the time young men and women are inducted into the army at age 18, the IDF has in hand all of their individual psychological and academic records. The IDF is notified of students with top grades, particularly in physics and math. Each September, 3,000 Talpiot candidates submit to a brain-busting battery of intellectual and scientific tests. They undergo heavy psychological profiling, and tests on leadership skills and their ability to work with others. By March, only 35 are left. 'The tests are so difficult, most people complete only 20 percent to 40 percent of

each exam,' says Assaf Monsa, a 29-year-old Talpiot graduate. 'Some of the questions are not solvable. They are not meant to be solved. It's to differentiate between the very good and the extraordinarily good.' Danziger says he's not sure even a known brain like Bill Gates could cut it. 'I think he could pass the ! intellectual part, but I don't know his human capabilities,' the major says. 'Is he pleasant to work with? Can he make other people do what he wants without financial authority?' (There's also the question of whether Gates would want to spend at least nine years in the military, as Talpiot graduates must. That's six years more than the minimum requirement for many other Israeli soldiers.) Talpiot soldiers spend the first three years and four months of their service housed in special barracks at Hebrew University in Jerusalem, where they undertake intensive study in cutting-edge science. They also go through eight months of basic training.

After graduation, they spend five years in the unit of their choice; almost all pick one of the elite technical units. 'These are the soldiers that all of the units want,' says Danziger.

Since Talpiot's inception, only a few hundred people have made it through the program. Their military handiwork is classified, although it is known to have touched everything from algorithm compression to antimissile systems. But Talpiot's role in the current tech boom is no secret. Assaf Monsa and another Talpiot graduate, Yair Mann, along with two other alumni of elite tech units, three years ago founded RichFX, which has developed streaming video technology that Monsa says uses between one-twentieth and one-hundredth of the bandwidth gobbled up by competing systems. (It's used by Neiman Marcus to sell $500-plus shoes over the Internet.) **Marius Nacht, another Talpiot grad, is a co-founder of Check Point.** Eli Mintz, CEO and president of Compugen, a gene sequencing technology firm, and Yuval Shalom, co-founder and CTO of Wiseband, a maker of wireless phone technologies, also went through Talpiot. 'The phrase 'It can't be done' is not for Talpiot,' says Ehud Ram, a recent! ly retired high-ranking intelligence officer who worked with some Talpiot grads over the years. (Ram's own background is in geophysics and remote sensing data. During a meeting three years ago, Ram informed Steve Ballmer, then Microsoft's second in command, that he should consider relocating the company's Redmond campus or risk being wiped out by a nearby long-dormant but still dangerous volcano. No word yet from Ballmer, now Microsoft's CEO.)" (Startup Nation by Stacy Perman) - http://www.timeinc.net/b2/subscribers/articles/print/0,17925,512689,00.html

"Graduates, along with those of other elite programs, are deployed throughout the armed services to do everything from reviving crashed computers to heading sophisticated military intelligence projects. Col. Albert Tregar's IDF programming school gets to choose the best, train them, and quickly put them into the field, where they could very well wind up practicing various forms of technological warfare." (Israeli Army Grads Lead Business Revolution by David Rosenberg) - http://www.cji.co.il/cji-n126.txt

MAMRAM

"Is the computer division of the IDF (Israel Defense Forces) in the areas of design and development of information systems. 1959 - MAMRAM, the Hebrew acronym for the IDF's Central Computing Facility, is formed.

MAMRAM is an abbreviation for Center of Computing and Information Systems; originally, Center of Computing and Mechanized Registration is the Israel Defense Forces' central computing system unit, providing data processing services for all arms and the general staff of the IDF. As of 2007, MAMRAM is under the command of Colonel Ayala Hakim.

In 1994, the MAMRAM programming school, considered one of the best sources of high-quality software professionals in the world, was separated into a newly-formed unit called BASMACH. However, the school's graduates, which were and still are highly sought after in the industry, are still referred to as MAMRAM graduates. Following graduation, BASMACH students go on to serve in various IDF units. Some of the graduates are often offered a position in MAMRAM itself." (MAMRAM - Wikipedia entry) - http://en.wikipedia.org/wiki/MAMRAM

"The demands of MAMRAM, another elite division, aren't as withering as Talpiot's — the MAMRAM washout rate is only 50 percent. MAMRAM, the Hebrew acronym for Central Unit for Data Processing, is the IDF's main computer corps, and trains all military software programmers and network systems architects.

MAMRAM candidates go through a six-month trial of up to 15-hour-a-day course work before they're admitted to the program. Those who make the grade must serve six years, minimum. Still, it is one of the most coveted postings in the military." (Startup Nation by Stacy Perman) - http://www.timeinc.net/b2/subscribers/articles/print/0,17925,512689,00.html

8-200

"Then there is 8-200, an electronic warfare unit founded in the early 1960s that many believe has left a bigger mark on the boom than any of Israel's other elite operations. Its name comes from its founding members: 8 Ashkenazi Jews and 200 Iraqi immigrants who were specialists in wireless communications and had worked for Iraqi Railways. Their skills became the cornerstone of the electronic intelligence gathering, encryption, and other activities known to be among the unit's specialties. It's illegal for past and present members to talk about 8-200, although it has become something of an open secret in the tech world. The unit has also attained a mythical status among venture capitalists for the entrepreneurial wizards who are veterans of the unit. Gil Shwed, one of Check Point's founders, allegedly served in 8-200, though he won't confirm that himself. 'I had the idea in the army, three years before I started Check Point,' Shwed says. 'I knew I had a good idea. If you can do it in the military environment, you have the tools to do it in other environments.'" (Startup Nation by Stacy Perman) - http://www.timeinc.net/b2/subscribers/articles/print/0,17925,512689,00.html

*Here's the confirmation:

"A four-year-long period goes virtually unmentioned in the official biography of the Israeli billionaire Gil Shwed. This much information can be cobbled together: In 1986 Shwed, just 18 years old, joined the supersecret electronic intelligence arm, Unit 8-200, of the Israeli Defense Forces. His job most likely was to string together military computer networks in a way that would allow some users access to confidential materials and deny it to others." (A Fortune in Firewalls by Lea Goldman) - http://members.forbes.com/global/2002/0318/042.html

The legend of the name is that unit began with eight Ashkenazis and 200 immigrants from Iraq. The Iraqi immigrants had previously worked on Iraqi Railways, knew wireless communications and of course, Arabic Israel Defense Force intelligence unit 8-200 may be Israel's greatest high-tech incubator, whose graduates have gone on to found companies like Check Point, NICE, Comverse and ECI. Israel Defense Force intelligence unit 8-200 may be Israel's greatest high-tech incubator, whose graduates have gone on to found companies like Check Point, NICE, Comverse and ECI. Not to mention all those start-ups. The Arena presents a first-ever expose of Israel's ultimate secret weapon.

“It began as a unit in the Intelligence Service of the Hagana (the pre-State underground army), called “Intelligence Service 2,” which was responsible for listening to enemy transmissions. 8-200 has undergone numerous incarnations. Today, it concentrates on intelligence gathering and decoding of encryption codes. It is a good and developed unit, whose contribution to the system is important. It was forbidden to talk about it for years. We have been hearing more about it recently and there have been a few publications in Israel and abroad. The unit recruits quality personnel, which then goes out and markets technologies developed there.”

“It is important to understand that this is a huge unit, that works in many fields. In general, it is responsible for all intelligence that can affect Israel’s security. Intelligence gathering in the unit comes from a variety of sources, i.e. listening to all types of broadcasts: telephones, fax, radio. The unit listens, intercepts and decodes information, mostly encrypted, though some is in clear.

“The major challenge is decoding encrypted transmissions. Unit computer experts and mathematicians are responsible for this, using mathematical models and algorithms.”

Yossi Melman, “Ha’aretz” Intelligence Affairs Correspondent and co-author of “Every Spy a Prince” says, “This is the most important intelligence unit in the State of Israel. More than the Mossad. The information obtained by this unit is of the highest priority to the entire intelligence community.” Melman continues, “In my opinion, many of the Israeli high-tech companies are based on the information amassed in the unit. But they are not exceptional. It happens everywhere. Not a few Mossad agents became businessmen after their retirement, using their connections and information amassed while in the service. There are suggestions of paying royalties to the State, but such suggestions reek of dictatorship.”

Alon of iWEB shows his courage, admitting, “It isn’t the paratroopers. There isn’t a strong social element. Guys come to work. In addition, the unit is strongly compartmentalized. If friendships developed, it was in small groups. Compartmentalization indeed. There is hardly any free movement at headquarters. Every soldier has authorization to enter only a few places, and each team is totally isolated from his neighbors. Military discipline is not rigidly enforced, apparently because there is no need for it. David of Power Dsine remembers, “I was scared when I arrived. I saluted the department head the first time I saw him. He told me that that would also be the last time.” (Nerds in Uniform by Batya Feldman) - http://web.archive.org/web/20041101081545/www.globes.co.il/DocsEn/did=387213.htm

"**1959** - Unit 8-200 of the Intelligence Corps is formed. Its first commander was Avraham Aloni, who in 1952 became the commander of the Signal Intelligence Unit of the IDF Intelligence Corps. Also in 1959, the electronics division was established which served as a research and technology division of the Intelligence Corps, which in turn became 8-200. E**ver since, graduates of 8-200 have gone on to hold leading positions in Israelâ's high-tech industries, becoming entrepreneurs and executives in such companies as Checkpoint, Comverse, Taldor, ECI Telecom, Audiocodes, Jacada, Compugen, Nice, and others."** (The 50s: Little Israel invents and devises by Dan Yachin) - http://www.globes.co.il/serveen/globes/docview.asp?did=487939&fid=1363

"Several of the founders of Israel's best-known tech success, the Internet security firm Check Point Software Technologies, are former members of 8-200 who specialized in developing firewalls between classified military computer networks." (Startup Nation by Stacy Perman) - http://www.timeinc.net/b2/subscribers/articles/print/0,17925,512689,00.html

MAMDAS

"Take the air force operational software and development center, known by its Hebrew acronym, MAMDAS. It designs some of the world's most sophisticated military software, and most of its personnel are in their early 20s. The key to its success, says Lieutenant Colonel Zafrir, an officer in the unit (the army censor prohibits publication of some officers' full names), lies in the close integration of development and operation and close cooperation between designers and people who use the technology in the field." (Israeli Army Grads Lead Business Revolution by David Rosenberg) - http://www.cji.co.il/cji-n126.txt

Unit 8153

The Mapping Unit, Modern Hebrew: Yehidat Mipui of the Israel Defense Forces military intelligence (Unit 8153) is in charge of strategic mapping of locations. It is known for doing so for both strategic and tactical purposes. (Mapping Unit - Wikipedia entry) - http://en.wikipedia.org/wiki/Mapping_Unit

***Okay, now that we've established the covert intelligence units of Israel, whose admitted roles are to recruit, train and place in the field or remotely, active service intelligence operatives. Whose acknowledged tasks were and are to intercept electronics communications, surreptitiously compromise the security of sensitive communications of targeted foreign countries, establish and insert "Trojan Horse" start-ups and spy software in strategic areas of secure electronic communications. For the purposes of compiling military and economic intelligence, then utilizing blackmail of individuals they find compromised through the electronic surveillance grid. This is technological warfare deployed against all they perceive as their enemies, and of foreign powers they can exploit to their advantage. Now let's examine some of the principle players and the 'front corporations they've established to carry out their covert and sanctioned espionage for Israel's military and interests! Again, I am using actual excerpts so that there may be no controversy regarding the veracity of statements.**

Check Point

"Gil Shwed is the data-security company's 34-year-old CEO. Fresh from his role as a network defense specialist for four years in the Israeli Defense Force, Shwed launched Check Point in 1993.

Check Point acquired Zone Labs in 2004. In October, 2005, Check Point announced it would acquire Sourcefire, the developers of Snort for $225 million. Both the Department of Defense and the FBI objected to the acquisition due to national security concerns. The acquisition was pending during an investigation by the Committee on Foreign Investment in the United States (CFIUS), but was announced to have collapsed over security concerns related to the "Snort" software which guards some classified U.S. military and intelligence computers.

The acquisition has been since withdrawn." (Wikipedia entry) - http://en.wikipedia.org/wiki/Check_Point

"Sourcefire is at work in leading financial, healthcare, manufacturing, technology and educational organizations throughout the U.S., Europe, Asia and Latin America.

But here is the kicker: Sourcefire solutions are trusted by all branches of the military, the largest civilian agencies, and domestic, internal and military intelligence organizations. This kicker has all the earmarks of a red flag, and that is exactly what came up. "We've decided to pursue alternative ways for Check Point and Sourcefire to partner in order to bring to market the most comprehensive security solutions," said Gil Shwed, Check Point's CEO." (Who Benefits From Check Point's Blocked Sourcefire Buyout?) -
http://software.seekingalpha.com/article/8479

So it seems that Mr. Shwed is on a mission both figuratively and literally, to get access to classified U.S. military and intelligence computers.

"Sourcefire makes network defense and intrusion detection software for an array of customers, including the Defense Department. The company has deep roots in the National Security Agency. Its founder and chief technology officer, Martin Roesch, has served as an NSA contractor. Its vice president of engineering, Tom Ashoff, developed software for the secretive spy agency." (U.S. Reviewing 2nd Dubai Firm) - http://www.washingtonpost.com/wp-dyn/content/article/2006/03/01/AR2006030102192_pf.html

"Sourcefire makes arguably the best network-based intrusion detection system that's ever existed, and it's used on some very sensitive networks by the US Government. Handing control of the company that develops and maintains that software to foreign interests seemed a little too much for the feds. "I think Sourcefire is a great company I think they had good things and I think I would be happy tohave them as a part of Check Point. But I don't think that there are no alternatives to that technology," Shwed says.

"Check Point will either form an OEM relationship with Sourcefire, or simply buy another company that owns a similar technology, he added. The roadmap stays the same, Shwed insists." (Check Point wants to be the last pure-play security vendor by Patrick Gray) -
http://www.zdnet.com.au/news/security/soa/Check-Point-wants-to-be-the-last-pure-play-security-vendor/0,130061744,139265693,00.htm

"Check Point has recently acquired Zone Labs, a company known for letting consumers download free software like Zone Alarm, a personal firewall. When asked if free software downloads will stop now with the acquisition, Mr Gil Shwed, chairman and CEO of Check Point, said: 'No, Zone Labs is doing a good job providing free products for consumers'."

"'The fact that it provides free products to people is a very good way to secure people and get them familiar with the need for security and also to test software programs. The fact that we have 25 million consumers is a great way to make sure that a product is tested in every environment'." (Check-ing on the Weakest) -

http://computertimes.asiaone.com/people/story/0,5104,1885,00.html

I find this statement troubling at least as much as I find the fact that they are producing Firewall software for personal computers, which any good intelligence technician would create with surreptitious back-door access installed.

Google

"Google was co-founded by Larry Page and Sergey Brin while they were students at Stanford University, and the company was first incorporated as a privately held company on September 7, 1998.

The first funding for Google as a company was secured in the form of a USD100,000 contribution from Andy Bechtolsheim, co-founder of Sun Microsystems, given to a corporation which did not yet exist. After viewing a quick demo, Sun Microsystems co-founder Andy Bechtolsheim (himself a Jewish immigrant from Germany) wrote a $100,000 check to 'Google, Inc.'" (The Story of Sergey Brin by Mark Malseed) -

http://www.momentmag.com/Exclusive/2007/2007-02/200702-BrinFeature.html

"Around six months later, a much larger round of funding was announced, with the major investors being rival venture capital firms Kleiner Perkins Caufield & Byers and Sequoia Capital. Sequoia Capital, one of the first Silicon Valley venture capital firms, has only one office outside the United States — **in Israel.** Financier Michael Moritz, from Sequoia currently sits on the board of Directors of Google. Google also owns both Google video and YouTube which was purchased in late 2006.

In 2004, Google launched its own free web-based email service, known as Gmail. **Google admits that deleted messages will remain on their system, and may be accessible internally at Google, for an indefinite period of time.**

For the first time in Google's history, the language in their new policy made it clear that they will be pooling all the information they collect on you from all of their various services.

Moreover, they may keep this information indefinitely, and give this information to whomever they warrant. Their corporate motto is "*Don't be evil*", and they even made sure that the Securities and Exchange Commission got this message in Google's IPO filing.

Google has never been known to delete any of the data they've collected, since day one. For example, their cookie with the unique ID in it, which expires in 2038, has been tracking all of the search terms you've ever used while searching their main index.

For all searches they record the cookie ID, your Internet IP address, the time and date, your search terms, and your browser configuration. Increasingly, Google is customizing results based on your IP number. This is referred to in the industry as 'IP delivery based on geolocation.'" (Compiled from various documented sources)

"Google has also developed Google Earth, an interactive mapping program powered by satellite imagery that covers the vast majority of the earth. Google Earth is generally considered to be remarkably accurate and extremely detailed. For example, some major cities have such remarkably detailed images that one can zoom in close enough and read the license plates on cars on a street. Specifically, some countries and militaries contend the software can be used to pinpoint with near-precision accuracy thephysical location of critical infrastructure, commercial and residential buildings, bases, government agencies, and so on." (Google Wikipedia entry) - http://en.wikipedia.org/wiki/Google

"Sergey Brins parents, Michael Brin, 59, a mathematics professor at the University of Maryland, and his wife, Eugenia, 58, is a research scientist at NASA's Goddard Space Flight Center. They are Jews who emigrated from Russia with the assistance of HIAS, the Hebrew Immigrant Aid Society, and $2,000 dollar loan from the Jewish community in Maryland. Google's first employee and a number of other early hires were Jewish and, when the initial winter holiday season rolled around, a menorah rather than a Christmas tree graced the lobby.

Like Sergey, Larry is the son of high-powered intellects steeped in computer science. His father, Carl Victor Page, a computer science professor at Michigan State University until his death in 1996, received one of the first Ph.D.s awarded in the field. His mother, Gloria, holds a master's degree in computer science and has taught college programming classes. The two young graduate students also shared a Jewish background." (The Story of Sergey Brin by Mark Malseed) -

http://www.momentmag.com/Exclusive/2007/2007-02/200702-BrinFeature.html

"DAVOS, Switzerland - Google 'is in the process of establishing an R&D center in Israel,' Sergey Brin, a founder of the Internet search titan, told Haaretz during the World Economic Forum here. Brin and co-founder Larry Page were among the more visible participants at the economic conference. Both have a solid connection with Israeli entrepreneurs in the Internet field." (Google plans Research and Development center in Israel) -

http://www.cji.co.il/cji-n301.txt

Google Facts:

"Matt Cutts, a software engineer at Google since January 2000, used to work for the National Security Agency. Keyhole, the satellite imaging company that Google acquired in October 2004, was funded by the CIA.

Keyhole is supported by In-Q-Tel, a venture capital firm funded by the CIA, in an effort to 'identify and invest in companies developing cutting-edge information technologies that serve United States national security interests.'

'We are moving to a Google that knows more about you.'" Google CEO Eric Schmidt, February 9, 2005 (Creepy Gmail) -

http://www.gmail-is-too-creepy.com/

"Both Google founders Sergey Brin and Larry Page attended Shimon Peres' 80th birthday extravaganza in September of 2003. Brin even spoke at a symposium entitled 'The Promise and Risk of Technology'" (Celebrating 80 Years with Shimon Peres) -

http://www.israelnewsagency.com/peres80.html

Onset Technology

"The problem is that BlackBerry's operating system includes only e-mail, an appointment book, and a contact list (personal information management). There are already several small software companies in the world that have discovered this vacuum, and are supplying added value services for BlackBerry's operating system. One of these companies is Israeli start-up Onset Technology Ltd., founded in 1997 by president and CEO Gadi Mazor and Ron Maor, both veterans of Unit 8-200 (the IDF signal intelligence gathering unit). Most of Onset Technology's current work involves the BlackBerry. The company's METAmessage software provides access to an enterprise's network via a BlackBerry. The software enables users to see files on an office computer, print them, and check for errors." (Bettering BlackBerry: Israeli Start-up Onset Technology will Develop Homeland Security Apps for Blackberry PDAs - by Ofer Levi) -

http://www.jgv.com/portfolio/port_onset2.htm

Odigo

"Odigo was an Israeli company whose headquarters were in New York, with offices in Herzliya. It offered instant messaging services via a minor messaging client called Odigo Messenger. Formally an affiliate web service provider Bravenet, Odigo was acquired by Comverse Technology on May 20, 2002. The founders of Odigo are Avner Ronen and his wife Maskit. Odigo is named after the Greek word for 'Guide'.

Avner, 24, would soon find himself living like a student in a battered East Village loft. He would see his fledgling company, Odigo, laid siege to by America Online, the user-friendly Godzilla of the Internet world. He would be poised to earn fantastic amounts of wealth — and would be equally poised to earn nothing. But having spent five years in the Israeli Defense Forces, he was not given to panic. 'Conflict with AOL is not so terrible,' he once told me. 'Things are more difficult with Hezbollah.' Ronen has never quite shed his military appearance — though having settled in Manhattan, and Banana Republic.

The Jan. 25 start-up of Odigo, which specializes in instant-message technology, was fast approaching. 'It may sound absurd in this Internet age,' he says, 'but sometimes you must physically be in an environment to feel what is happening. You need presence.' Choosing Silicon Alley over Silicon Valley was a matter of pure logistics: Odigo had 70 employees back home, and Ronen believed that the extra time difference between Israel and California would be too burdensome.

Still in the cab, Avner called Israel and casually informed his wife, Maskit, of his impulse to move. She agreed instantly. Maskit, who is also 24, met Avner in the military, where she had a senior rank and, significantly, was his computer instructor. (She is now one of Odigo's software engineers.) 'There was no time to digest this information for either of us,' Avner recalls. 'Moving here was just a theory.'" (Immigrants with an I.P.O. by Marshall Sella) - http://partners.nytimes.com/library/magazine/home/20000917mag-sella.html

"Odigo came into the news in the aftermath of the September 11 attacks, because two workers claimed that they received word of an upcoming terrorist attack two hours in advance, via their own messaging service. The two employees allegedly recorded the ip-address and notified the authorities after the attack. [1]" (Wikipedia entry) - http://en.wikipedia.org/wiki/Odigo

"Odigo, the instant messaging service, says that two of its workers received messages two hours before the Twin Towers attack on September 11, predicting the attack would happen, and the company has been cooperating with Israeli and American law enforcement, including the FBI, in trying to find the original sender of the message predicting the attack.

Micha Macover, CEO of the company, said the two workers received the messages and immediately after the terror attack informed the company's management, which immediately contacted the Israeli security services, which brought in the FBI.

Odigo usually zealously protects the privacy of its registered users, said Macover, but in this case the company took the initiative to provide the law enforcement services with the originating Internet Presence address of the message, so the FBI could track down the Internet Service Provider, and the actual sender of the original message." (Odigo says Workers were warned of attack by Yuval Dror) - http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=77744&contrassID=/has%5C

"Odigo, Inc., founded in 1998, is a leading provider of Instant Messaging and Presence Solutions to wireless carriers and service providers worldwide with a community of over 8M users world wide. Odigo's products include IM servers, SMS-IM gateways, and presence management solutions. **On May, 2002 Odigo was Aquired by Comverse**, the world's leading supplier of software and systems enabling network-based multimedia enhanced communications services. The field-proven Odigo Instant Messaging service, which serves millions of subscribers, enables Comverse to expand its offering to include both in-network and outsourced Instant Communications Solutions. http://www.odigo.com/

"AOL aol (nyse: aol - news - people) last weekend blocked the latest version of the Odigo Messenger from working with AOL Instant Messenger (AIM).

Late Monday, Odigo figured out a way around the blockade, but early today AOL again put the kibosh on Odigo's software.

Both companies say they're ready for a long battle. AOL contends that by accessing its servers, Odigo is compromising AOL's security and risking the privacy of AIM users.

AOL spokeswoman Tricia Primrose was equally adamant: 'We're not going to allow unauthorized access to our servers. No doubt they will try to devise a new workaround, and then we'll block them again.'" (AOL Again Blocks Odigo by David Einstein) - http://www.forbes.com/2000/06/13/mu5.html

Does anyone else think this is abusive technical hacking into AOL's servers who clearly don't want them there and feel it would compromise the security and personal records of AOL users? If this AOL was a woman and Odigo a man, he would be guilty of stalking, harassment and repetitive date rape. What do you call a company that forces its services and products on you whilst attempting to gain access to confidential consumer data? Oh that's right a spy op.

"Shortly after 9-11, Odigo was completely taken over by Comverse Technology, which had been part owner of Odigo since early 2000, if not earlier. Shortly after 9/11, five executives from Comverse were reported to have profited by more than $267 million from 'insider trading.'

Avner Ronen, the 'founder' of Odigo, was Vice President of Business Development of Comverse Technology in October 2005. This indicates that Ronen and Kobi Alexander (of Comverse), both Israeli military officers with computer backgrounds, have been close business partners since early 2000.

'Comverse and Odigo have had a long-standing partnership and together have developed instant communications products and services that we have recently begun to offer to operators around the world,' Zeev Bregman, CEO of the Israel-based Comverse Ltd., told *The Jerusalem Post* in May 2002. (Why was Kobi Alexander Allowed to Flee?) - http://www.iamthewitness.com/Bollyn-Kobi-Alexander.html

Gilat Satellite Networks

Made more than half of the interactive VSATs (Very Small Aperture satellite Terminals), or small satellite earth stations used in communications networks sold in the world.

"(06/13/2006 10:03 AM EDT)
ZICHRON YAACOV, Israel - Satellite maker Gilat Satellite Networks said its technology will be incorporated into Cisco Systems' routers. Gilat's touts its SkyEdge technology as allowing Cisco routers to supply integrated services and the capacity to securely transmit high-speed voice, video and data services. The move is designed to provide an alternative communications path in parallel with terrestrial communications." (Cisco to Cooperate with Gilat for Satellite Backup) - http://www.eetimes.com/showArticle.jhtml?articleID=189400601

"Like many others in the Israeli high tech field, Yoel Gat is a graduate of the Intelligence Corps, and a protege of Zohar Zisappel. He entered the civilian job market in 1987 only because he did not win against Eric Paneth in the stand-off for the position of unit commander. Three years later, Paneth became one of the founders of Orckit.

Gilat Satellite Networks subsidiary Gilat Communications, set up in Israel under the management of Shlomo Tirosh, is increasingly becoming a major factor in the Israel inland communications market, and like its parent company, was highly successful in issuing on Wall Street. Gilat grew from being a start-up to a 500-staff company, which constantly shows profits (generally exceeding expectations), and never ceases to innovate in satellite communications. Gat stands at the head of the pyramid of a company with a hush-hush aura attached to it by a team of guys who left the Intelligence Corps and globally conquered the satellite communications market.

Leaving the unit together with Gat were Amiram Levinberg, his brother Joshua Levinberg, Shlomo Tirosh and Gideon Kaplan, and together they set up Gilat Satellite Networks (GILTF)." (Yoel Gat - Gilat Satellite Networks, The Hush-hush Guy by Efi Landau) - http://web.archive.org/web/20041125013723/www.globes.co.il/DocsEn/did=381329.htm

ECTel

"ECtel, a unit of telecoms equipment holding firm ECI Telecom, makes monitoring equipment for communications networks. In August of 2003, a major unnamed telecoms carrier had ordered the Israeli company's lawful Interception application. A valuation for deal was not given and a spokeswoman for the firm declined to comment on the size of the contract. For those who may not be familiar with the term 'lawful interception' it is more commonly known as wiretapping." (Israel ECtel wins U.S. telecoms carrier deal) - http://www.forbes.com/technology/newswire/2003/08/19/rtr1061040.html

From ECTel's own website it states that Chairman of the Board Yair Cohen, "served as Brigadier General of Unit 8-200, the central military intelligence unit of the Israeli Defense Forces." It further elaborates that "in this capacity, he was engaged in the development of state-of-the-art military technology." (ecTel.com) - http://www.ectel.com/content.aspx?id=367

Narus

"Narus is a private company founded in 1997 by Ori Cohen, who had been in charge of technology development for VDONet, an early media streaming pioneer.

It is notable for being the creator of NarusInsight, a supercomputer system which is used by the NSA and other bodies to perform mass surveillance and monitoring of citizens' and corporations' Internet communications in real-time, and whose installation in AT&T's San Francisco Internet backbone gave rise to a 2006 class action lawsuit by the Electronic Frontier Foundation against AT&T.

In 2004, Narus engaged the former Deputy Director of the National Security Agency, William Crowell as a director. From the Press Release announcing this:

‘Crowell is an independent security consultant and holds several board positions with a variety of technology and technology-based security companies. Since 9/11, Crowell has served on the Defense Advanced Research Projects Agency (DARPA) Task Force on Terrorism and Deterrence, the National Research Council Committee on Science and Technology for Countering Terrorism and the Markle Foundation Task Force on National Security in the Information Age.’” (Narus Wikipedia entry) - http://en.wikipedia.org/wiki/Narus

“One of the devices in the ‘Cabinet Naming’ list is particularly revealing as to the purpose of the ’secret room’: a Narus STA 6400. Narus is a 7-year-old company which, because of its particular niche, appeals not only to businessmen (it is backed by AT&T, JP Morgan and Intel, among others) but also to police, military and intelligence officials. Last November 13-14, for instance, Narus was the ‘Lead Sponsor’ for a technical conference held in McLean, Virginia, titled ‘Intelligence Support Systems for Lawful Interception and Internet Surveillance.’ Police officials, FBI and DEA agents, and major telecommunications companies eager to cash in on the ‘war on terror’ had gathered in the hometown of the CIA to discuss their special problems. Among the attendees were AT&T, BellSouth, MCI, Sprint and Verizon. Narus founder, Dr. Ori Cohen, gave a keynote speech. So what does the Narus STA 6400 do?

‘The (Narus) STA Platform consists of stand-alone traffic analyzers that collect network and customer usage information in real time directly from the message…. These analyzers sit on the message pipe into the ISP (internet service provider) cloud rather than tap into each router or ISP device’ (Telecommunications magazine, April 2000). A Narus press release (1 Dec., 1999) also boasts that its Semantic Traffic Analysis (STA) technology ‘captures comprehensive customer usage data … and transforms it into actionable information…. (It) is the only technology that provides complete visibility for all internet applications.’

The next logical question is, what central command is collecting the data sent by the various ’secret rooms’? One can only make educated guesses, but perhaps the answer was inadvertently given in the DOD Inspector General’s report (cited above):

‘For testing TIA capabilities, Darpa and the U.S. Army Intelligence and Security Command (INSCOM) created an operational research and development environment that uses real-time feedback. The main node of TIA is located at INSCOM (in Fort Belvoir, Virginia)… .”

Among the agencies participating or planning to participate in the INSCOM ‘testing’ are the ‘National Security Agency, the Defense Intelligence Agency, the Central Intelligence Agency, the DOD Counterintelligence Field Activity, the U.S. Strategic Command, the Special Operations Command, the Joint Forces Command and the Joint Warfare Analysis Center.’ There are also ‘discussions’ going on to bring in ‘non-DOD federal agencies’ such as the FBI.” (AT&T Whistle-Blower’s Evidence by Wired) - http://www.commondreams.org/headlines06/0517-10.htm

“If you’ve been keeping track of American Internet and the battles over surfer privacy, then you have run into the name Narus, which specializes in tapping surfer traffic. It was founded in 1997 by Dr Ori Cohen, Stas Khirman and four other guys in Israel.

For years Narus sailed on untroubled. But today it’s become associated with the likes of Carnivore or Echelon, the notorious software programs that have become linked with spying on email and delivering data on surfers to government agencies.

The image change Narus has suffered and its frequent mentions in debates on privacy and the freedom of information, is mainly because of Mark Klein. That would be a technician retired from AT&T for 22 years, who reported to the American authorities a few months ago that he suspected AT&T of allowing the National Security Agency to bug its customers’ phone calls.

Customer Internet traffic via the WorldNet service provider was reportedly shunted to data-mining technology in a secret room at AT&T facilities. The data analysis technology was made by Narus.

It is very possible that Cohen and Khirman are working at a startup that nobody is willing to talk about. A stealthy startup they helped found called Cright that has lots of employees in Israel and California, and which is reportedly about to avail itself of Ukrainian development talent too. Almost nobody has heard of Cright and nobody at all, including its distinguished investors, is willing to discuss what it does.

Sequoia Israel, the Rolls Royce of the technological venture capital world, is whispered to have invested $7 million in Cright together with Charles River. But the enigmatic startup is not mentioned on the Sequoia site, which otherwise describes the portfolio very thoroughly. Nor does the Charles River site mention it.

Nor could I glean any information about the company or about the Narus people manning it. Cright has a website, a naked one that reveals nothing: and has taken a vow of utter silence.

Market sources surmise that Cright is tight-lipped because what it does would spark outrage among surfers jealous of their privacy, which could culminate in migraines for the startup and its backers.

But that is assuming that Ori Cohen and Stas Khirman are still working on products that analyze Internet traffic, and possibly, that this time their prying eye is looking at private surfers.

Industry sources in the know claim they're harnessing Israeli developers to develop a DRM product designed for installation at Internet providers, which will among other things frustrate file sharing and peer-2-peer networks. These sources say Cright (could that be short for copyright?) is supposed to filter P2P networks, to monitor and analyze files being shared, and possibly to shut down errant P2P network, or at least to block certain content.

In other words, if may be a new twist on the old trick of monitoring the Internet's main line, analyzing content, and interfering with it, just as Narus says it does in Saudi Arabia." (Ori Cohen, Private Eye by Raphael Fogel) - http://www.haaretz.com/hasen/pages/ArticleContent.jhtml?itemNo=737258

You have Narus, established to collect internet intel on American citizens for the NSA, DIA, CIA, DHS and a host of others within the US intelligence community. What don't they want you to know beyond that? Well, Narus was founded by Israeli native Ori Cohen in 1997, prior to that he was the VP of Business and Technology Development for VDOnet, a leading provider of Internet video conferencing and video on demand software solutions. Prior to VDOnet, he served as CEO for IntelliCom Ltd.

So both Narus and later companies Skyrider and CRight were founded by a shadowy Israeli citizen with substantial U.S. intelligence connections named Ori Cohen. But Cohen's bio doesn't go beyond his work in the UK with Intellicom Ltd. UK, the rest has been aggressively sanitized and filtered. No picture, and absolutely no information beyond Intellicom Ltd. which I find most unusual. But I'm going to go out on a limb and wager that what are the odds that U.S. telecom traffic is being compromised by at least 3 Israeli intel fronts, and then the NSA's internet monitoring own capacities just happen to be farmed out to yet another Israeli founded company with tenuous intel connections?

Evidence at this level, you think, would make this extremely suspicious to any agency pledged to defend the country against foreign espionage. Yet here before all, it not only doesn't raise an eyebrow, but they've actually instituted the espionage by allowing a foreign power access to all of their sensitive data! One can only wonder at the extortion and blackmail material these Israeli companies have amassed that's being used against powerful figures within the U.S. to sanction this level of insanity. But in thinking this out further, maybe there's something more.

Because by using these Israeli cut-out contractors, the U.S. agencies can effectively bypass those troublesome domestic surveillance laws and other legal obstacles, by utilizing foreign intelligence agencies such as in Israel to collect the data for them. So, the Israeli intelligence can amass extortion and blackmail material to force any leaders with something to hide, to supporting their wars and agenda. Whilst the U.S. can illegally collect net profiles, histories and whatever from any Joe and Jane citizen they want to, and reserve any incriminating or useful information for further use down the road.

Comverse Technology, Inc. (a.k.a Comverse Infosys & Verint)

"Comverse Infosys designs, develops, manufactures and markets advanced telecommunications processing solutions for telecommunications carriers and Law Enforcement Agencies. Solutions include the acquisition, storage, processing and analysis of voice, data and video electronic communications. The open-ended, modular designs provide the versatility to easily adapt new technologies and enhancements to meet future requirements, such as 3G Cellular and packet data networks." (Comverse Infosys Profile) - http://cryptome.org/verint-spysys.htm

"Founded in 1981, the company focuses on providing services to third party telecommunication service providers. The real parent company of Comverse was Jacob 'Kobi' Alexander's Tel Aviv-based Efrat Future Technology Ltd., which carried out 'all research, development, and manufacturing,' for Comverse. (Wikipedia entry) - http://en.wikipedia.org/wiki/Comverse_Technologyhttp://en.wikipedia.org/wiki/Comverse_Technology)

"The latest incarnation known as Verint Systems defines itself as a global organization providing analytic software solutions for communications interception, digital video security and surveillance, and enterprise business intelligence. We generate actionable intelligence through the collection, retention and analysis of video, email, Internet and data transmissions from multiple types of communications." (Crytome.org) http://cryptome.org/verispy.htm

"CARL CAMERON, FOX NEWS CORRESPONDENT: The company is Comverse Infosys, a subsidiary of an Israeli-run private telecommunications firm, with offices throughout the U.S. It provides wiretapping equipment for law enforcement. Here's how wiretapping works in the U.S.

Every time you make a call, it passes through the nation's elaborate network of switchers and routers run by the phone companies. Custom computers and software, made by companies like Comverse, are tied into that network to intercept, record and store the wiretapped calls, and at the same time transmit them to investigators. The manufacturers have continuing access to the computers so they can service them and keep them free of glitches. This process was authorized by the 1994 Communications Assistance for Law Enforcement Act, or CALEA. Senior government officials have now told Fox News that while CALEA made wiretapping easier, **it has led to a system that is seriously vulnerable to coundermined the whole wiretapping system.**

Congress [sic, probably Comverse] insists the equipment it installs is secure. But the complaint about this system is that the wiretap computer programs made by Comverse have, in effect, a back door through which wiretaps themselves can be intercepted by unauthorized parties.

Adding to the suspicions is the fact that in Israel, Comverse works closely with the Israeli government, and under special programs, gets reimbursed for up to 50 percent of its research and development costs by the Israeli Ministry of Industry and Trade. But investigators within the DEA, INS and FBI have all told Fox News that to pursue or even suggest Israeli spying through Comverse is considered career suicide.

And sources say that while various F.B.I. inquiries into Comverse have been conducted over the years, they've been halted before the actual equipment has ever been thoroughly tested for leaks. A 1999 F.C.C. document indicates several government agencies expressed deep concerns that too many unauthorized non-law enforcement personnel can access the wiretap system. And the FBI's own nondescript office in Chantilly, Virginia that actually oversees the CALEA wiretapping program, is among the most agitated about the threat.

But there is a bitter turf war internally at F.B.I. It is the FBI's office in Quantico, Virginia, that has jurisdiction over awarding contracts and buying intercept equipment. And for years, they've thrown much of the business to Comverse. A handful of former U.S. law enforcement officials involved in awarding Comverse government contracts over the years now work for the company. Numerous sources say some of those individuals were asked to leave government service under what knowledgeable sources call "troublesome circumstances" that remain under administrative review within the Justice Department."

"CAMERON: Beyond the 60 apprehended or detained, and many deported since Sept. 11, another group of 140 Israeli individuals have been arrested and detained in this year in what government documents describe as "an organized intelligence gathering operation," designed to "penetrate government facilities." Most of those individuals said they had served in the Israeli military, which is compulsory there.

But they also had, most of them, intelligence expertise, and either worked for Amdocs or other companies in Israel that specialize in wiretapping. Earlier this week, the Israeli embassy in Washington denied any spying against or in the United States" (Transcripts of Fox News Special Report with Brit Hume, from December 13, 2001) - http://www.whatreallyhappened.com/israeli_spyring_fox.html and http://cryptome.org/fox-il-spy.htm

CARL CAMERON, FOX NEWS CORRESPONDENT: Los Angeles, 1997, a major local, state and federal drug investigating sours. The suspects: Israeli organized crime with operations in New York, Miami, Las Vegas, Canada, Israel and Egypt. The allegations: cocaine and ecstasy trafficking, and sophisticated white-collar credit card and computer fraud. The problem: according to classified law enforcement documents obtained by Fox News, the bad guys had the cops' beepers, cell phones, even home phones under surveillance. Some who did get caught admitted to having hundreds of numbers and using them to avoid arrest.

'This compromised law enforcement communications between LAPD detectives and other assigned law enforcement officers working various aspects of the case. The organization discovered communications between organized crime intelligence division detectives, the FBI and the Secret Service.'

Shock spread from the DEA to the FBI in Washington, and then the CIA. An investigation of the problem, according to law enforcement documents, concluded, 'The organization has apparent extensive access to database systems to identify pertinent personal and biographical information.'" (Transcripts of Fox News Special Report with Brit Hume, from December 14, 2001) - http://www.whatreallyhappened.com/israeli_spyring_fox.html and http://cryptome.org/fox-il-spy.htm

"Another Israeli telecom company is Comverse Infosys, which subcontracts the installation of the automatic tapping equipment now built into every phone system in America. Comverse maintains its own connections to all this phone tapping equipment, insisting that it is for maintenance purposes only. However, Converse has been named as the most likely source for leaked information regarding telephone calls by law enforcement that derailed several investigations into not only espionage, but drug running as well." (The Israeli Spy Ring) - http://www.whatreallyhappened.com/spyring.html

"Comverse is one of the most notable companies involved in the options backdating scandal. The Ex-CEO of Comverse, Jacob Alexander, an Israeli citizen, has been classified as a wanted fugitive from August 2006 by the American Federal Bureau of Investigation. Along with former finance chief David Kreinberg and former senior general counsel William Sorin, Alexander faces multiple charges of conspiracy, securities fraud, wire fraud, mail fraud, money laundering and making false filings to the Securities and Exchange Commission; all of these charges relate to alleged options backdating or other actions related to stock options. **Jacob "Kobi" Alexander, was an Israeli military officer connected to the Odigo instant messaging company whose employees and users received an early warning of the 9/11 attacks, has become a fugitive from U.S. justice and taken refuge in Israel along with other prime suspects of the terror attacks."** (Wikipedia entry) -

http://en.wikipedia.org/wiki/Comverse_Technology

"BEIJING, Sept. 28, 2006 (Xinhuanet) — Securities fraud fugitive Jacob "Kobi" Alexander, former Comverse Technology Inc. chief executive officer, was arrested Wednesday in Namibia.

Alexander, 54, former Israeli intelligence officer turned high-technology entrepreneur, will be brought before a court in Windhoek within 48 hours, and the U.S. will seek his extradition, the Justice Department said.

Federal prosecutors charged Alexander on Aug. 9 with backdating stock options to boost the compensation of executives at New York-based Comverse, the world's largest maker of voicemail software.

'Alexander's alleged role in options backdating victimized Comverse shareholders and deceived prospective investors,' Brooklyn U.S. Attorney Roslynn Mauskopf said in a statement. 'The fraud affected the company's bottom line by misstating earnings.'

After Alexander was charged and fled the U.S. the FBI put his face on its Most Wanted list and Interpol initiated a global 'red notice,' asking police to arrest the former CEO. Prosecutors said today that Alexander isn't a U.S. citizen as the FBI stated in a press release after he was first charged.

Robert Nardoza, a spokesman for Mauskopf, said the former CEO, a citizen of Israel, is also a permanent resident of the U.S.

Alexander wired 57 million U.S, dollars to Israel in July from an account at Citigroup Inc.'s Smith Barney Unit, the U.S. government said, calling the transfer an effort to 'aunder the proceeds of the fraud.' His assets in two Citigroup Smith Barney accounts were frozen July 31.

A 32-count indictment unsealed Wednesday by Garaufis in Brooklyn federal court charged Alexander with crimes relating to an alleged 'slush fund" and the backdating of stock options from 1998 to 2006. He is charged with conspiracy, securities fraud, making false filings with the U.S. Securities and Exchange Commission, mail fraud, wire fraud and money laundering." (Fugitive: Interpol arrests Jacob Alexander) - http://news.xinhuanet.com/english/2006-09/28/content_5149944.htm

Comverse Technology, the U.S.-based 'parent company' of an older and much bigger Israel-based company with the same name, is the owner of the Verint, Ulticom, Starhome, Mercom and Startel companies.

Alexander, was recently allowed to flee the United States after he and two other former Comverse executives were charged with securities, mail and wire fraud by U.S. prosecutors in Brooklyn, New York. A warrant has been issued for his arrest. While a spokesman for the U.S. Attorney's office for the Eastern District of New York told AFP on August 15 that he 'expected' that Alexander would turn himself in, The New York Times was rather less optimistic. 'It will be a long time - if ever - before Alexander explains himself in a courtroom,' the Times wrote on August 21. Alexander's lawyer, Robert Morvillo, said he 'believed' that Alexander and his family were on vacation in Israel. Alexander, an Israeli citizen and a former military officer, wired $57 million to an account in Israel at the end of July and was evidently allowed to flee the United States.

'Given Alexander's stature and military service,' the Times reported, quoting unnamed law professors, 'Israel might be reluctant to readily hand him over.' One might reasonably ask, 'What does the 54-year old Alexander's 'military service' have to do with Israel refusing to extradite him for crimes committed in the United States?'

While Alexander is obviously connected with Israel's military intelligence apparatus and George Soros through the mutually owned investment fund ComSor, what is not widely reported is his company's close links with Odigo, the Israeli-run instant messaging company that received - and conveyed - urgent warning messages about the imminent terror attacks on the World Trade Center, several hours before the first plane hit." (Why was Kobi Alexander Allowed to Flee?) -

http://www.iamthewitness.com/Bollyn-Kobi-Alexander.html

AmDocs Limited

"Headquarters in St. Louis, Missouri but primarily based in Ra'anana, Israel, is a provider of software and services for billing, CRM (Customer Relationship Management) and OSS (Operational Support Systems) systems. Its clients are primarily focused on the telecommunications, including such "Tier-1" players as Comcast, Cablevision, DirecTV, Jupiter Communications, Cable One, Sprint-Nextel, Cingular, Vodafone, T-Mobile and Sensis.

The company was originally called 'Aurec Group' (the Hebrew word for Artery, which in Hebrew is used to describe a communication channel) and dealt only with directory services, i.e. Yellow Pages. They now provide application suites for CRM, sales, and billing operations for telecommunication service providers. Amdocs still provides publishing software for creating print and online directories. The company also offers outsourced customer service and data center operations. Amdocs claims to be the largest billing system's software and services provider in the world.; in the USA, they provide billing and directory assistance for 90% of the phone companies.

As of 2002, Dov Baharav replaced Avi Naor, as Amdocs' CEO." (Wikipedia entry) - http://en.wikipedia.org/wiki/Amdocs

"CARL CAMERON, FOX NEWS CORRESPONDENT: Here's how the system works. Most directory assistance calls, and virtually all call records and billing in the U.S. are done for the phone companies by Amdocs Ltd., an Israeli-based private telecommunications company. Amdocs has contracts with the 25 biggest phone companies in America, and more worldwide. The White House and other secure government phone lines are protected, but it is virtually impossible to make a call on normal phones without generating an Amdocs record of it.

In recent years, the FBI and other government agencies have investigated Amdocs more than once. The firm has repeatedly and adamantly denied any security breaches or wrongdoing. But sources tell Fox News that in 1999, the super secret National Security Agency, headquartered in northern Maryland, issued what's called a Top Secret sensitive compartmentalized information report, TS/SCI, warning that records of calls in the United States were getting into foreign hands in Israel, in particular. Investigators don't believe calls are being listened to, but the data about who is calling whom and when is plenty valuable in itself. An internal Amdocs memo to senior company executives suggests just how Amdocs generated call records could be used.

"Widespread data mining techniques and algorithms…. combining both the properties of the customer (e.g., credit rating) and properties of the specific 'behavior…. '" Specific behavior, such as who the customers are calling. The Amdocs memo says the system should be used to prevent phone fraud. But U.S. counterintelligence analysts say it could also be used to spy through the phone system. Fox News has learned that the N.S.A has held numerous classified conferences to warn the F.B.I. and C.I.A. how Amdocs records could be used. At one NSA briefing, a diagram by the Argon national lab was used to show that if the phone records are not secure, major security breaches are possible.

Another briefing document said, 'It has become increasingly apparent that systems and networks are vulnerable… Such crimes always involve unauthorized persons, or persons who exceed their authorization…citing on exploitable vulnerabilities.' Those vulnerabilities are growing, because according to another briefing, the U.S. relies too much on foreign companies like Amdocs for high-tech equipment and software. Fox News has documents of a 1997 drug trafficking case in Los Angeles, in which telephone information, the type that Amdocs collects, was used to 'completely compromise the communications of the FBI, the Secret Service, the DEA and the LAPD.'

BRIT HUME, HOST: Last time we reported on an Israeli-based company called Amdocs Ltd. that generates the computerized records and billing data for nearly every phone call made in America. As Carl Cameron reported, U.S. investigators digging into the 9/11 terrorist attacks fear that suspects may have been tipped off to what they were doing by information leaking out of Amdocs." (Transcripts of Fox News Special Report with Brit Hume, from December 11-14, 2001) - http://www.whatreallyhappened.com/israeli_spyring_fox.html and http://cryptome.org/fox-il-spy.htm

"Amdocs Limited was founded by Avi Naor. Avi served in the Israeli army, and holds a BSC degree in computer sciences from the Technion Israel Institute of Technology. In 1976 he joined the Aurec Group, and in 1982 he founded Amdocs.

Naor also founded an organization by the name of Mahal2000 and serves as it's director. Mahal is the Hebrew acronym for "Overseas Volunteers" and is a non-profit organization dedicated to enabling young (ages 18-23) overseas Jews to volunteer for service in the IDF, followed by a commitment to Jewish community service in their country of origin. Mahal2000 cooperates directly with the IDF, Ministry of Interior and many others in order to facilitate the enlistment of overseas volunteers. What this smells like is an active global training programme for spies, including their deployment overseas at conclusion. It even spells out specifically what non-Jews can do for the programme in this following excerpt obtained here: http://www.mahal2000.com/about/non-Jewish-volunteer.htm.

"Since then however, the policy has been to restrict service in the armed forces to citizens of Israel, Jews as well as Christians, Moslems, Druze and others, and to non-Israeli Jews so as to avoid placing at risk persons who do not have this connection to Israel. In addition, the maximum enlistment date limit is the 23rd birthday for men and the 20th for women. Unfortunately no exception can be made.

You have the opportunity, however, to take your place defending Israel on the 'public relations front'. Today, wars and battles are often won or lost on TV screens, in the minds and hearts of good people. Therefore, public relations is no less important than planes and tanks. You could, for example, volunteer to be a PR Ambassador of Middle-East-Info.org and explain to others what it means for Israel to be the sole democracy in a region comprising 23 dictatorships (including 5 out of the world's 7 state sponsors of terrorism and about half of the world's major terror groups).

Of the 19 most repressive regimes in the world, 7 are in Arab states and Iran. Arab regimes and Iran are also a breeding ground for advocating Jihad (Holy War) against all non-Muslims (Christians, Hindus, Buddhists, Animists and Jews included) and openly seek world domination and the ultimate destruction of freedom." The very nature of this enterprise confirms the fact that Avi Naor is very currently active in military circles within Israel. Also of note regarding Amdocs, is that Israeli spies using the cover as "art students'

were arrested for gaining access into the offices and even the homes of federal law enforcement agents and government officials. Thirteen in all were busted and the two principals of the operation were Itay Simon and Michael Calmanovic, who were bailed out immediately by Amdocs employee Ophir Baer, who posted their $50,000 bond.

While in custody, Simon told his interrogators that he "did classified work for the Israeli army." According to the report, "Simon refused to answer questions about his military service" As for Calmanovic, he stated that he was a recently discharged "electronic intercept operator for the Israeli military". **One striking fact stands out, and that is the large number of "art students" who were experts in the art of handling explosives. What were these guys doing during their stay in this country before it was so rudely interrupted by the feds or, rather, what were they preparing to do? (Leaked Government Report Exposes Israeli Spy Ring by Justin Raimondo) -** http://www.antiwar.com/justin/j032202.html

http://www.washington-report.org/backissues/072000/0007043.html

More than two dozen U.S. intelligence, counterintelligence, law-enforcement and other officials have told Insight that the FBI believes Israel has intercepted telephone and modem communications on some of the most sensitive lines of the U.S. government on an ongoing basis. The worst penetrations are believed to be in the State Department. But others say the supposedly secure telephone systems in the White House, Defense Department and Justice Department may have been compromised as well.

The problem for FBI agents in the famed Division 5, however, isn't just what they have uncovered, which is substantial, but what they don't yet know, according to Insight's sources interviewed during a year-long investigation by the magazine. Of special concern is how to confirm and deal with the potentially sweeping espionage penetration of key U.S. government telecommunications systems allowing foreign eavesdropping on calls to and from the White House, the National Security Council, or NSC, the Pentagon and the State Department.

This discovery by Division 5 should have come as no surprise, given what its agents had been tracking for many months. But the FBI discovered enough information to make it believe that, somehow, the highest levels of the State Department were compromised, as well as the White House and the NSC.

According to Insight's sources with direct knowledge, other secure government telephone systems and/or phones to which government officials called also appear to have been compromised.

As for how this may have been done technologically, the FBI believes it has uncovered a means using telephone-company equipment at remote sites to track calls placed to or received from high-ranking government officials, possibly including the president himself, according to Insight's top-level sources. One of the methods suspected is use of a private company that provides record-keeping software and support services for major telephone utilities in the United States.

A local telephone company director of security Roger Kochman tells Insight, "I don't know anything about it, which would be highly unusual. I am not familiar with anything in that area".

U.S. officials believe that an Israeli penetration of that telephone utility in the Washington area was coordinated with a penetration of agents using another telephone support-services company to target select telephone lines. Suspected penetration includes lines and systems at the White House and NSC, where it is believed that about four specific phones were monitored — either directly or through remote sites that may involve numbers dialed from the complex.

"[The FBI] uncovered what appears to be a sophisticated means to listen in on conversations from remote telephone sites with capabilities of providing real-time audio feeds directly to Tel Aviv", says a U.S. official familiar with the FBI investigation. Details of how this could have been pulled off are highly guarded. However, a high-level U.S. intelligence source tells Insight: "The access had to be done in such a way as to evade our countermeasures … That's what's most disconcerting."

Despite elaborate precautions by the U.S. agencies involved, say Insight's sources, this alleged Israeli intelligence coup came down to the weakest link in the security chain: the human element.

The technical key appears to be software designs for telephone billing records and support equipment required for interfacing with local telephone company hardware installed in some federal agencies. The FBI has deduced that it was this sophisticated computer-related equipment and software could provide real-time audio feeds. In fact, according to Insight's sources, the FBI believes that at least one secure T-1 line routed to Tel Aviv has been used in the suspected espionage.

The potential loss of U.S. secrets is incalculable. So is the possibility that senior U.S. officials could be blackmailed for indiscreet telephone talk. Many officials do not like to bother with using secure, encrypted phones and have classified discussions on open lines. (Insight Magazine - FBI Probes Espionage at Clinton White House By J. Michael Waller and Paul M. Rodriguez) - http://www.spongobongo.com/zy9850.htm

Also of interest is the fact that the Chief Operations Officer (COO) of Amdocs in 2003 was a man named Sami Totah. Totah is a veteran of Israel's military intelligence group Unit 8-200 and is now the Eternal Director of ECTel.

Vuance Ltd. formerly SuperCom

VUANCE Ltd. (formerly SuperCom) is an established Solution Provider, providing its customers with innovative Incident Management, Asset Management, e-ID solutions. (Vuance.com) - http://www.vuance.com/SiteFiles/1/765/3283.asp

SuperCom, Ltd. is engaged in research, development and marketing of advanced technologies and products for smart-card solutions and government e-ID projects. SuperCom offers a wide range of standard and customized smart card-based solutions for physical and logical security, education, corrections facilities and air & seaports. SuperCom is also a leader in the manufacturing of secure and durable documents such as national identity cards, passports, visas, drivers' licenses and vehicle registration. Together with its subsidiaries, SuperCom offers advanced, innovative and flexible solutions in contact and contactless smart-card technologies. Headquartered in Israel, SuperCom has subsidiaries in the US and Hong Kong.

New York, NY, and Raanana, Israel, October 11, 2004 — SuperCom, Ltd. (Euronext: SUP) a leading smart card and e-ID technology integrator and solutions provider serving governmental and commercial markets, announced today that the United States Government Printing Office (GPO) has informed that the Company's proposal as a prime contractor for the integration of smart card technology in the US new electronic passports has been accepted for award.

This project is considered to be the largest and most advanced smart passport project in the world to date. The US authorities have announced multiple awards for the implementation of the project that will include the production of smart inlay for the new passports with a sophisticated chip containing personal identification such as biometric data This type of passport will be difficult to forge and will replace the traditional passport that contained a printed personal photograph and was considered to be easy to falsify. The scope of the project based on the RFP is estimated at 50 million passports over the following five years.

In this project, SuperCom will supply the smart card technology that it has developed over the recent years including the smart chip with an operating system and antenna that is embedded in the passport. (SuperCom Wins Tender for the Integration of Technology in the United States Smart Passport) - http://cc.msnscache.com/cache.aspx?q=8275198176058&lang=en-US&mkt=en-US&FORM=CVRE

KADIMA, Israel — " SuperCom Ltd. has unveiled new technology for active tracking of people and assets.

The Israeli provider of smart card and electronic identification products has developed movement detection technology that can monitor and track numerous items simultaneously. The tracking technology employs small, low-powered RF tags attached to an object or a person. License-free radio bands are used to track the RF band from a programmable transmitter.

SuperCom claims its Pure RF product can monitor and locate tagged items using a hand-held tracking device, which can also be integrated into cellphones.

With an eye on the U.S. homeland security market, the company has appointed former CIA Director R. James Woolsey as chairman of its advisory board. (Tracking Technology could have Homeland Defense Apps by Joel Bainerman) - http://www.eetimes.com/news/semi/showArticle.jhtml?articleID=180204127

R. James Woolsey served as Director of Central Intelligence from 1993-1995.

He is currently Vice President of Booz Allen Hamilton's Global Strategic Security practice. Woolsey previously served on the National Commission on Terrorism. He was Under Secretary of the Navy, Ambassador to the Negotiation on Conventional Armed Forces in Europe (CFE), and was General Counsel to the U.S. Senate Committee on Armed Services.

Woolsey was appointed by President Reagan as Delegate at Large to the U.S.-Soviet Strategic Arms Reduction Talks (START), and the Nuclear and Space Arms Talks (NST). He also was an Advisor with the U.S. Delegation to the Strategic Arms Limitation Talks (SALT I). Woolsey served on the President's Commission on Defense Management, President's Commission on Federal Ethics Law Reform, and President's Commission on Strategic Analysis.

He was a Captain in the U.S. Army and was a staff member for the National Security Council.

Mr. Woolsey is a graduate of Stanford (Phi Beta Kappa), holds an M.A. from Oxford University (where he was a Rhodes Scholar), and received a L.L.B. from Yale Law School (where he was Managing Editor of the Yale Law Journal). (Vuance.com) - http://www.vuance.com/SiteFiles/1/764/3280.asp

*As persistent and as diligently as I tried, I could find nothing on the backgrounds of either Supercom or Vuance's founders as of this writing. All search results were heavily sanitized and filtered from any of the numerous entries I tried to locate them on. Also, please bear in mind that any of the links I've posted could be taken down at any time by the very parties who wish this information to remain covert.

July 26th, 2007