Israeli Computer Spying Linked to 'X Committee'

by Edward Spannaus

A computer espionage scandal with ties into the United States and Britain is wracking Israel, with top executives from a number of major Israeli companies, and employees from three private detective agencies, having been placed under arrest. The probe centers on the use of "Trojan Horse" computer software to spy on other companies and to steal secret computer data from them.

According to a well-informed Israeli with ties to the intelligence community, the Trojan Horse operation was also used to penetrate the British MI-6 intelligence service, and U.S. intelligence agencies, and is linked to the "Amdocs" operation which *EIR* had exposed shortly after the 9/11 attacks, in our investigation of the Israeli "art students" spy network operating in the United States.

On May 31, the Israeli press reported that top officials of Israeli telecommunications giants Amdocs and Bezeq International were marched into police stations in Tel Aviv for questioning. An Amdocs official acknowledged using one of the private investigators implicated in the Trojan Horse case, but claimed that it was all for legitimate purposes.

The spy scandal began last November, after police discovered that Michael Haephrati, a London-based Israeli who developed his computer skills during three years with the Israeli military, had developed a computer program which could penetrate target computers without being detected by anti-virus systems, and then transmit data from those computers to others. Some sources believe that Haephrati is using an updated version of PROMIS, a "trap door" spying program that was stolen from a U.S. software company, Inslaw, by the Justice Department during the Reagan Administration.

The scope of the current investigation is continually expanding. "Right now, it is a very sophisticated investigation," Tel Aviv police superintendent Peal Liat was quoted by the London-based *Computer Weekly* as saying. "We have something like 150 different computers that were taken by investigators. Every computer they open, they discover more. Every day it gets us more companies that ordered the information, and more companies that were infected."

"They were able to see everything, from e-mails to documents to information," Liat said. "And they were able to copy it and take it out. We think the Trojan had the ability to log

keystrokes." Images and documents were sent to FTP servers in Israel, Germany, and the United States, *Computer Weekly* reports.

Amdocs and the 'Art Students'

Although the Israeli investigation is being portrayed as one involving industrial espionage, Amdocs has previously been implicated in much more sinister operations in the United States.

- In 1997, Amdocs was involved in the installation of a new telephone system in the White House, in what is believed to have been part of the "X Committee" operations targetting President Bill Clinton (see preceding article). According to reports which surfaced in the U.S. press in the Spring of 2000, the FBI was investigating the operation, in which supposedly secure White House telephone discussions were being intercepted and transmitted to Tel Aviv. It was reported at that time that the FBI had sought an arrest warrant for an Amdocs employee, but it was quashed by the Justice Department.
- Following the 9/11 attacks, *EIR* and others reported on the three-year investigation being conducted by the U.S. Drug Enforcement Administration (DEA) of the Israeli "art student" ring, which had implicated Amdocs in a number of ways. Many of the "art students" carrying out surveillance of U.S. security and military facilities, had entered the U.S. with work permits listing Amdocs as their employer. The DEA documented efforts by the "students" to profile law enforcement and military personnel for prospective recruitment by Israel.
- The DEA suspected that Amdocs, which provides billing services to the 25 largest phone companies in the United States—and thus had access to records of almost every telephone call dialed in the country—was providing counter-surveillance information to Israeli mafia drug-trafficking circles about the actions of law-enforcement agencies, and about wiretaps placed on targets of law-enforcement investigations.
- In the wake of the 9/11 attacks, U.S. law enforcement personnel established that a number of the Israel "students"—many of whom had specialized training in the Israeli military—were also infiltrating Arab-American communities, and lived in close proximity to some of the 9/11 hijackers. Others had long-established connections to suspected Islamic terrorist cells.

As we reported in our profile of Amdocs in the Feb. 1, 2002 issue of *EIR,* the senior managers of Amdocs are reported to be senior members of the Israeli military and intelligence services. The company is still very secretive. The Israeli business publication *Globes* reported on May 31, 2005, in connection with the Trojan Horse investigation: "Although Amdocs is a public company, it shies away from the media. Amdocs' managers have never given interviews, the company is parsimonious with information, and often behaves like a covert organization."