The Washington Post

# ARGENTINE, 22, CHARGED WITH HACKING COMPUTER NETWORKS

By Pierre Thomas; Elizabeth Corcoran
March 30, 1996

After an elaborate federal investigation in cyberspace, law enforcement officials have charged a young Argentine with using the Internet to illegally break into sensitive computer networks at Department of Defense installations, the National Aeronautics and Space Administration, Los Alamos National Laboratory and several universities.

Justice Department officials are seeking the arrest of Julio Cesar Ardita, 22, of Buenos Aires, who they said illegally entered Harvard University computers via the Internet and from there invaded other networks containing confidential, but not classified, research files on such things as aircraft design, radar technology and satellite engineering.

The case marked the first time federal authorities had secured a court order to monitor private electronic communications.

Prosecutors say they are continuing to investigate what Ardita might have done with the information he gained access to by tapping into computers in the United States, Brazil, Chile, Korea and Taiwan. Under the provisions for computer fraud, Ardita cannot be extradited to the United States, but Argentine officials also are considering charges against him for misusing telecommunications equipment.

Ardita, during a brief telephone conversation in Argentina, declined to discuss the charges and instead put his father, Julio Rafael Ardita, on the line. "We have not done anything here," Julio Rafael Ardita said. "I don't know what the FBI is talking about."

When Julio Rafael Ardita was read the list of computer systems his son allegedly broke into, he said that if they were vulnerable to a relatively modest personal computer, then perhaps something was wrong with the security systems in the United States.

"These Yankees don't have the slightest idea about security. Who is at fault?" he asked. "Obviously, the North Americans are not very clear on the security of their systems if a kid from South America can enter them. I would be ashamed to admit it."

Although computer hackers have broken into supposedly secure computer systems in the past, government investigators on this occasion aggressively tracked down a suspect while taking pains to safeguard the privacy of thousands of other users.

Prosecutors called the investigation a preview of a coming era of "cyber-sleuthing," when federal agents will spend the bulk of the their time sitting at computer terminals navigating through a web of electronic leads to catch computer criminals, rather than knocking on doors and sifting through paperwork.

"This is . . . a glimpse of what computer crime-fighting will look like in the coming years," said Donald K. Stern, U.S. Attorney for the Massachusetts District.

Law enforcement officials said the case also underscored the vulnerability of computer systems worldwide. In recent months, government officials have wrestled with industry executives and privacy advocates over rules governing the use of encryption technology, used for scrambling information.

"This case demonstrates that the real threat to computer privacy comes from unscrupulous intruders, not government investigators," said Attorney General Janet Reno.

The tale begins last August, when managers at the Naval Command, Control and Ocean Surveillance Center in San Diego discovered in their computer system several innocuous-looking files with names like "sni256" and "test." The managers did not know who had stored them. But when they opened up the files, they found a "sniffer" program, used to copy vital information, such as passwords supplied by legitimate users when they log into the system.

All Navy investigators could tell was that whoever had installed the sniffer programs had used a computer system at Harvard University to enter their computer. But over the next few weeks, Navy managers in other locations, including Arlington, as well as officials in the Army Research Labs in Edgewood, Md., began spotting similar sniffer programs in their systems. These, too, had been planted by a Harvard-based computer. In September, managers at the Army Research Labs in Aberdeen reported that a Harvard computer had unsuccessfully tried to get into its computer system about 90 times.

Investigators began to see links when they realized that the sniffer programs and related files were often stored under similar names, including "zap" and "pinga." According to the National Computer Crime Squad, none of these file names had been used by hackers in quite the way this intruder seemed to use them.

In mid-November, federal agents obtained court orders to set up a monitoring program to check communications coming into key Harvard computers. The law requires that agents try to keep their eavesdropping to a minimum. Of the 10 million bits of information per second that could flow through the Harvard network, law enforcement officers only wanted to find the few that might contain the telltale signs of the intruder.

They created a filter that would pick up only messages that contained the file names and other account information they had discovered in the sites that had been invaded. Once the suspicious communications were stored, federal officials electronically sifted through them as many as four more times, trying to winnow out communications that didn't match the hacker's profile.

Over two months, investigators put together a portrait of the hacker: where and when the intruder had slipped into computer systems, how many times sniffer programs had been set up, and so on. The trail led to Telecom Argentina and, officials say, to Ardita.

On Dec. 28, Argentine officials seized Ardita's computer files and equipment. Yesterday, U.S. officials formally charged him with violating federal law. He will be arrested if he attempts to visit the United States.

Federal agents have done electronic surveillance of traffic over computer networks in the past, but only with the consent of users or when computer networks had posted a banner telling users that their communications might be moni tored. Because the Harvard network had no such warning, federal authorities on this occasion sought a court order to eavesdrop in cyberspace.

"I anticipate that appropriate court-ordered surveillance . . . will be used in like vein in the future," Reno said.

The case occurs at a time when the government is confronting growing questions about how well its traditional techniques for tracking and stopping criminals work in the digital era. Industry, privacy advocates and, most recently, some members of Congress have contended that law enforcement officials are so eager to ensure that they can electronically eavesdrop that they effectively are preventing U.S. citizens and companies from using tough digital locks to protect private information.

"The case shows that there's a need for more encryption," said David Banisar, policy analyst at the Electronic Privacy Information Center. "If you had better security for these systems, you wouldn't have had the break-ins in the first place."

But law enforcement officials argued that the case shows federal investigators can effectively wield electronic tools for tracking down digital trespassers, without violating other users' privacy. "This is an example of how the Fourth Amendment {guaranteeing the right to privacy} and a court order can be used to protect rights while adapting to modern technology," Reno said. Correspondent Gabriel Escobar in Buenos Aires contributed to this report. CAPTION: THE HACKER'S PATH 1. Ardita uses PC and modem to crack Telecom Argentina and other Argentine Internet systems. 2. Ardita breaks into Harvard, and through Harvard, into Internet systems around the world, including : NASA Jet Propulsion Laboratory Taiwan Ministry of Education South Korean engineering institute University of Sonora, Mexico Sao Paulo, Brazil, medical school Chilean corporation Naval Command, Control and Ocean Surveillance Center Two other Massachusetts universities Los Alamos National Laboratory Telecom Argentina Naval Research Laboratory SOURCE: Justice Department

For more on how we manage comments and other feedback, please see our **discussion and submission guidelines**